МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий інститут автоматики і електротехніки

Кафедра комп'ютерних технологій та інформаційної безпеки

ЗАТВЕРДЖУЮ
Завідувач кафедри комп'ютерних технологій та інформаційної безпеки, к.т.н., доцент
_____С.М. Нужний
«18» 06 2025 р.

Кваліфікаційна робота
на правах рукопису

КВАЛІФІКАЦІЙНА РОБОТА

РОЗРОБКА ШАБЛОНУ КСЗІ ДЛЯ ОБ'ЄКТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ВОДНОГО ТРАНСПОРТУ

Ступінь вищої освіти: БАКАЛАВР
Галузь знань: 12 «Інформаційні технології»
Спеціальність: 125 «Кібербезпека та захист інформації»
Освітньо-професійна програма: Системи технічного захисту інформації, автоматизація її обробки

Виконала: студентка 4 курсу групи 4387зст
Білостоцька Діана Михайлівна

Кваліфікаційна робота містить результати самостійного виконання навчального завдання. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Білостоцька Д.М.

Керівник: викладач кафедри комп'ютерних технологій та інформаційної безпеки **Трибулькевич Вікторія Вікторівна** _____

Миколаїв – 2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий інститут автоматики і електротехніки

ЗАТВЕРДЖУЮ
Гарант освітньої програми,
к.т.н., доцент, завідувач кафедри КТІБ
_____С.М. Нужний
«_18_» ____ос_____ 2025 р.

ЗАВДАННЯ

на кваліфікаційну роботу

Студентка: Білостоцька Діана Михайлівна

Курс:4

Група: 4387зст

Ступінь вищої освіти: бакалавр

Галузь знань: 12 Інформаційні технології

Спеціальність: 125 «Кібербезпека та захист інформації»

Освітньо-професійна програма: Системи технічного захисту інформації, автоматизація її обробки

1. Тема роботи: «Розробка шаблону КСЗІ для об'єкта інформаційної діяльності водного транспорту»
затверджена наказом НУК від «_23__» _квітня_____2025 р. № УЧ- 343

2. Вихідні дані до роботи: нормативно-правова база кібербезпеки та захисту інформації об'єктів інформаційної діяльності (ОІД) в галузі водного транспорту та розробки комплексних систем захисту інформації (КСЗІ), теоретичні основи управління інформаційною безпекою і побудови захищених баз даних

провести аналіз відкритих літературних джерел і визначити склад бібліотеки нормативно-правових актів і рекомендацій стосовно КСЗІ ОІД у галузі водного транспорту; визначити склад документів, які мають бути оформлені в процесі створення КСЗІ ОІД, провести аналіз їх структури, визначити типові для них і повторювані блоки інформації та розробити шаблони документів

4. Терміни виконання завдання:
термін видачі завдання: «_03_» _лютого_ 2025 р.
термін подання роботи: «_18_» _червня_ 2025 р.

5. План-графік виконання кваліфікаційної роботи

№ п/п	Заходи	Дата		Готовність	Відмітка про виконання
		Навч. тиждень	Контрольна дата		
10.	Організаційні збори.	23	03.02.2025	Вибір теми, визначення мети, завдань, об'єкта та предмета дослідження	
11.	Організаційні збори	25	20.02.2025	Попередній варіант оглядових розділів, підбір і опрацювання списку використаних джерел	
12.	Рубіжний контроль	31	03.04.2025	Попередній варіант повної КР.	
13.	Рубіжний контроль	33	20.04.2025	Попередній варіант презентації.	
14.	ЄДКІ на рівень «бакалавр»	34	29.04.2025	Здавання ЄДКІ зі спеціальності на ступінь бакалавра	
15.	Перевірка на плагіат	42	14.06.2025	1. Електронний варіант кваліфікаційної роботи; 2. Подання КР на перевірку на плагіат.	
16.	Кафедральний захист	43	18.06.2025	1. Оформлена КР (в форматі pdf) (передається студентом на кафедрі для внутрішньої рецензії, висновок керівника). У разі отримання позитивної внутрішньої рецензії, КР подається на зовнішню рецензію. 2. Оформлена презентація (в форматі pdf).	
17.	Подання документів на захист	44	24.06.2025	1. Подання щодо захисту КР 2. Зовнішня рецензія (окремо від КР). Резюме на КР. 3. Висновок кафедри про КР, допуск до захисту; 4. Електронний варіант та роздрукована презентація в кількості 5 примірників. 5. Електронний варіант КР на диску	
18.	Захист КР	44	25.06.2025	1. Приєднання студента до засідання кваліфікаційної комісії (конференції) у встановлений час для проведення процедури дистанційного захисту 2. Процедура захисту КР.	

ПРИМІТКА: Завдання додається до виконаної роботи та подається до атестаційної комісії.

Керівник
Викладач кафедри комп'ютерних технологій
та інформаційної безпеки _____ В.В. Трибулькевич

Студентка _____ Д.М.Білостоцька

АННОТАЦІЯ

Білостоцька Д.М. Розробка шаблону КСЗІ для об’єкта інформаційної діяльності водного транспорту. – Кваліфікаційна робота на правах рукопису.

Кваліфікаційна робота на здобуття ступеня вищої освіти «бакалавр» за спеціальністю F5 «Кібербезпека та захист інформації» галузі знань F «Інформаційні технології», освітньо-професійна програма «Системи технічного захисту інформації, автоматизація її обробки». – Національний університет кораблебудування імені адмірала Макарова, Миколаїв, 2025.

Пояснювальна записка: 131 с., 52 рис., 103 посилання.

Кваліфікаційна робота присвячена актуальній темі – розробці засобів автоматизації процесів створення комплексних систем захисту інформації (КСЗІ) об’єктів критичної інфраструктури. Об’єктом дослідження в даній роботі є КСЗІ. Предметом дослідження є проектна документація для створення КСЗІ на об’єкті інформаційної діяльності водного транспорту. Методами дослідження є аналіз відкритих літературних джерел, теоретичні основи управління інформаційною безпекою та побудови захищених баз даних. Метою роботи є розробка шаблонів документів для КСЗІ об’єкта інформаційної діяльності водного транспорту з урахуванням чинних нормативно-правових актів.

В роботі проведено аналіз відкритих літературних джерел і визначений склад бібліотеки нормативно-правових актів та рекомендацій стосовно КСЗІ ОІД у галузі водного транспорту; визначений склад документів, які мають бути оформлені в процесі створення КСЗІ ОІД; проведено аналіз структури документів, які мають бути оформлені в процесі створення КСЗІ ОІД, визначені типові для них і повторювані блоки інформації та розроблені шаблони документів.

Робота має практичне значення, оскільки її результати можуть бути використані в навчальному процесі зі спеціальності F5 «Кібербезпека та захист інформації» і при проектуванні КСЗІ у галузі водного транспорту.

Ключові слова: критична інфраструктура, водний транспорт, комплексна система захисту інформації, нормативно-правове забезпечення, шаблони документів.

ANNOTATION

Bialostotska D.M. Development of a CIPS template for the object of water transport information activities. – Qualification work in the form of a manuscript.

Qualification work on receiving a higher education degree "Bachelor" in the specialty F5 "Cybersecurity and Information Protection" of the field of knowledge F "Information Technologies", educational and professional program " Systems technical protection of information, automation of its processing" - Admiral Makarov National University of Shipbuilding, Mykolaiv, 2025.

Explanatory note: 131 pp., 52 figs., 103 references.

Qualification work is devoted to a topical issue – the development of means of automating the processes of creating complex information protection systems (CIPS) of critical infrastructure objects. The object of research in this work is CIPS. The subject of research is the design documentation for the creation of CIPS at an object of information activity (OIA) of water transport. The research methods are the analysis of open literary sources, theoretical foundations of information security management and the construction of secure databases. The purpose of the work is to develop document templates for the CIPS of the object of information activity of water transport, taking into account current regulatory legal acts.

In thesis an analysis of open literary sources have been carried out and the composition of the library of regulatory legal acts and recommendations regarding the CIPS OIA in the field of water transport have been determined; the composition of documents that must be drawn up in the process of creating the CIPS OIA have been determined; an analysis of the structure of documents that must be drawn up in the process of creating the CIPS OIA have been carried out, typical and repetitive blocks of information for them have been determined and document templates have been developed.

The work has practical significance, since its results can be used in the educational process in the specialty F5 "Cybersecurity and Information Protection" and in the design of CIPS in the field of water transport.

Keywords: critical infrastructure, water transport, comprehensive information protection system, regulatory and legal support, document templates.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

BIMCO – Baltic and International Maritime Council (Балтійська і міжнародна морська рада);

CIWIN – Critical Infrastructure Warning Information Network (інформаційна мережа попередження про критичну інфраструктуру);

CSA – Chamber of Shipping of America (Судноплавна палата Америки);

CSIRT – Computer Emergency Response Team (мережа груп реагування на інциденти з комп'ютерною безпекою);

DCSA – Digital Container Shipping Association (Асоціація цифрових контейнерних перевезень);

ENISA – European Union Agency for Network and Information Security (Агентство Європейського Союзу з питань мережевої та інформаційної безпеки);

EPCIP – European Programme for Critical Infrastructure Protection (Європейська програма захисту критичної інфраструктури);

EU- CyCLONe – European Cyber Crisis Liaison Organization Network (мережа зв’язку організацій з європейських кіберкриз);

GDPR – General Data Protection Regulation (Загальний регламент захисту даних);

IACS – International Association of Classification Societies (Міжнародна асоціація класифікаційних співтовариств);

IAPH – International Association of Ports and Harbours (Міжнародна асоціація портів та гаваней);

ICS – International Chamber of Shipping (Міжнародна палата судноплавства);

IMO – International Maritime Organization (Міжнародна морська організація);

INTERCARGO – International Association of Dry Cargo Shipowners (Міжнародна асоціація власників суховантажних суден);

IMCA – International Marine Contractors Association (Міжнародна асоціація морських підрядників);

INTERTANKO – International Association of Independent Tanker Owners (Міжнародна асоціація незалежних власників танкерів);

ISM code – International Safety Management code (Міжнародний кодекс з управління безпекою, МКУБ)

ISPS code – International Ship and Port Facility Security Code (Міжнародний кодекс охорони суден і портових засобів, Кодекс ОСПЗ)

IUMI – International Union of Marine Insurance (Міжнародний союз морського страхування);

MTS-ISAC – Maritime Transportation System Information Sharing and Analysis Center (Центр обміну та аналізу інформації та системи морського транспорту, США);

MSC – Maritime Safety Committee (Комітет з морської безпеки *IMO*);

NCI – National Critical Infrastructure (національна критична інфраструктура);

NIS – Network and Information Security Directive (Директива мережевої та інформаційної безпеки);

NIST – United States National Institute of Standards and Technology's (Національний інститут стандартів і технологій США);

NORMA Cyber – Nordic Maritime Cyber Resilience Centre (Північний морський центр кіберстійкості);

OCIMF – Oil Companies International Marine Forum (Міжнародний морський форум нафтових компаній;

OECD – Organisation for Economic Co-operation and Development (Організація економічного співробітництва та розвитку);

SOLAS – International convention for the Safety Of Life At Sea (Міжнародна конвенція з охорони людського життя на морі)

Sybass – Superyacht Builders Association (Асоціація будівельників супер'яхт);

USAID – United States Agency for International Development (укр. Агентство міжнародного розвитку США);

WSC – World Shipping Council (Всесвітня рада судноплавства);

ДІР – державні інформаційні ресурси;

ДССЗЗІ – Державна служба спеціального зв’язку та захисту інформації;

ЄКІ – європейська критична інфраструктура;

ЗІ – захист інформації;

ІзОД – інформація з обмеженим доступом;

ІКС – інформаційно-комунікаційна система;

ІКТ – інформаційно-комунікаційна технологія;

ІТ – інформаційна технологія;

ІС – інформаційна система;

КЗЗ – комплекс засобів захисту;

КЗІ – криптографічний захист інформації;

КІ – критична інфраструктура;

КСЗІ – комплексна система захисту інформації;

КТЗІ – комплекс технічного захисту інформації;

МКУБ – Міжнародний кодекс з управління безпечною експлуатацією суден і запобіганням забрудненню;

НД – нормативний документ;

ОІД – об’єкт інформаційної діяльності;

ОКІ – об’єкт критичної інфраструктури;

ОКІІ – об'єкт критичної інформаційної інфраструктури;

ОСПЗ – охорона суден і портових засобів;

ОТ – операційна технологія;

СБІ – система безпеки інформації;

СБУ – Служба безпеки України;

СУІБ – система управління інформаційною безпекою;

СУБ – система управління безпекою;

ТЗІ – технічний захист інформації.

ВСТУП

Дана кваліфікаційна робота присвячена актуальній темі – розробці засобів автоматизації процесів створення комплексних систем захисту інформації (КСЗІ) об’єктів критичної інфраструктури. Актуальність даної роботи зумовлена збільшенням в усіх галузях людської діяльності, в тому числі і у галузі водного транспорту, об’єктів інформаційної діяльності (ОІД), де озвучується і циркулює інформація з обмеженим доступом (ІзОД) різних ступенів секретності, для яких постає задача створення комплексу технічного захисту інформації (КТЗІ) і КСЗІ.

Створення КСЗІ для ОІД в загальному випадку регламентується низкою нормативних документів (НД) з технічного захисту інформації (ТЗІ) [62-72]. У галузі водного транспорту розробка, впровадження та експлуатація КСЗІ ускладнюється необхідністю враховувати галузеві вимоги щодо захисту комп’ютеризованих суднових систем, суден, портів, проектувальних організацій в галузі суднобудування, суднобудівних та судноремонтних підприємств і вимоги великої кількості інших стейкхолдерів [10, 14, 15, 18-20, 73, 102, 103]. В галузі морського та внутрішнього водного транспорту чинними є також нормативно-правові акти, що стосуються захисту критичної інфраструктури (КІ) [2, 9, 13, 15, 23, 24, 49, 84, 86, 91, 95, 96], нормативні документи низки міжнародних галузевих організацій та їх рекомендації щодо впровадження в галузі найкращих галузевих світових практик з кібербезпеки та захисту інформації [3-6, 11, 12, 16, 17]. Таким чином, при створення КСЗІ у галузі водного транспорту необхідно враховувати обов’язкові до виконання вимоги і бажано враховувати рекомендації (можливо – вибірково), що містяться у множині документів, на які необхідно робити посилання. З іншого боку, документація, яка оформлюється на КСЗІ є типовою. Тому для прискорення процесу створення КСЗІ водного транспорту і уникання помилок видається доцільним застосувати засоби автоматизованої обробки інформації з відповідною інформаційною підтримкою.

Метою даної роботи є розробка шаблонів документів для КСЗІ об’єкта інформаційної діяльності водного транспорту з урахуванням чинних нормативно-правових актів.

Досягнення цієї мети вимагає виконання наступних завдань:

− провести аналіз відкритих літературних джерел і визначити склад бібліотеки нормативно-правових актів і рекомендацій стосовно КСЗІ ОІД у галузі водного транспорту;

− визначити склад документів, які мають бути оформлені в процесі створення КСЗІ ОІД;

− провести аналіз структури документів, які мають бути оформлені в процесі створення КСЗІ ОІД, визначити типові для них і повторювані блоки інформації та розробити шаблони документів.

Об’єктом дослідження в даній роботі є КСЗІ.

Предметом дослідження в даній роботі є проектна документація для створення КСЗІ на ОІД водного транспорту.

Методами дослідження є аналіз відкритих літературних джерел, теоретичні основи управління інформаційною безпекою та побудови захищених баз даних.

1 АНАЛІЗ НОРМАТИВНО-ПРАВОВИХ АКТІВ І РЕКОМЕНДАЦІЙ СТОСОВНО КСЗІ ОІД У ГАЛУЗІ ВОДНОГО ТРАНСПОРТУ

1.1 Законодавчі акти щодо створення КСЗІ у галузі водного транспорту

1.1.1 Закон України «Про захист інформації в інформаційно-комунікаційних системах»

Закон України «Про захист інформації в інформаційно-комунікаційних системах» в редакції від 20.04.2025 [93] в статті 10 визначає, що:

а) Кабінет Міністрів України:

−встановлює базовий профіль безпеки, тобто мінімальні вимоги до захисту «систем, власниками або розпорядниками яких є органи державної влади, державні органи, державні підприємства, установи та організації, органи місцевого самоврядування, в яких обробляються державні інформаційні ресурси» [93] або ІзОД, вимога щодо захисту якої встановлена законом (крім вимог до забезпечення захисту інформації (ЗІ) у сфері надання платіжних, банківських та інших фінансових послуг, які визначає Національний банк України (див. п. д)»;

−визначає порядок затвердження базових, цільових та галузевих профілів безпеки;

−затверджує порядок проведення підтвердження відповідності КСЗІ, авторизації з безпеки;

б) Адміністрація Державної службу спеціального зв’язку та захисту інформації (ДССЗЗІ), яка згідно [77] є спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації:

−здійснює контроль за забезпеченням захисту, визначає вимоги та порядок створення КСЗІ державних інформаційних ресурсів (ДІР) або ІзОД, вимога щодо захисту якої встановлена законом;

– організовує проведення державної експертизи КСЗІ, експертизи та підтвердження відповідності засобів технічного захисту інформації (ТЗІ) і криптографічного захисту інформації (КЗІ);

– здійснює методичне керівництво підтвердженням відповідності КСЗІ, авторизацією з безпеки та забезпечує їх реалізацію (у порядку, проведення, встановленому Кабінетом Міністрів України);

– затверджує порядок ведення і веде перелік авторизованих систем з безпеки;

– розробляє та затверджує базовий профіль безпеки «для відповідної категорії інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем» [93], в яких обробляються ДІР (у порядку, встановленому Кабінетом Міністрів України);

в) органи державної влади, державні органи, органи місцевого самоврядування «розробляють та затверджують цільові профілі безпеки для інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем, власником або розпорядником яких вони є» [93] з урахуванням:

– базового профілю безпеки;

– стандартів;

– політик безпеки;

– призначення системи;

– структурно-функціональних характеристики системи;

– результати аналізу ризиків безпеки;

– особливостей функціонування системи;

г) органи державної влади, державні органи в межах своїх повноважень у певній галузі або сфері розробляють та за погодженням із ДССЗЗІ затверджують галузеві профілі безпеки з урахуванням:

– базового профілю безпеки;

– стандартів;

– політик безпеки;

−галузевих особливостей функціонування системи;

д) Національний банк України встановлює всі вимоги (всі профілі безпеки - базові, галузеві та/або цільові) щодо забезпечення ЗІ, у сфері, де він здійснює державне регулювання та нагляд (надання платіжних, банківських та інших фінансових послуг, валютне регулювання та валютний нагляд, депозитарний обліку Національного банку України);

е) Міністерство оборони України та Служба безпеки України, «розробляють і затверджують галузеві та/або цільові профілі безпеки для інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, власником (розпорядником) яких є Міністерство оборони України та/або Збройні Сили України і Служба безпеки України. в порядку, встановленому Кабінетом Міністрів України» [93].

Закон України «Про захист інформації в інформаційно-комунікаційних системах» із змінами, внесеними згідно Закону України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об’єктів критичної інформаційної інфраструктури» [84] встановлює, що КСЗІ та системи управління інформаційною безпекою (СУІБ) з підтвердженою відповідністю, створені до 20.04.2025 р. не потребують повторного підтвердження відповідності (авторизації).

1.1.2 Закон України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об’єктів критичної інформаційної інфраструктури»

Згідно Закону України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об’єктів критичної інформаційної інфраструктури» [84], який набув чинності з 20.04.2025 р., були внесені зміни в наступні закони:

−Закон України «Про захист інформації в інформаційно-комунікаційних системах» [93];

– Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»;

– Закон України «Про стандартизацію»;

– Закон України «Про основні засади забезпечення кібербезпеки України» [97].

Закон [84] має на меті ефективне інтегрування України у глобальну систему кіберзахисту, підвищення стійкості цифрових систем України до сучасних викликів шляхом імплементації до національного законодавства норм європейських директив з кібербезпеки, які стосуються організації і функцій команд реагування, впровадження найкращих практик обміну повідомленнями про кіберінциденти і управління ризиками.

На сайті ДССЗЗІ [83] серед важливих змін та нововведень, передбачених Законом України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури», називаються:

– «відмова від КСЗІ та визначення процесу впровадження заходів з управління ризиками і забезпечення того, щоб такі заходи підтримувалися протягом життєвого циклу систем на основі профілів безпеки;

– функціонування системи оцінювання стану кіберзахисту включно з методом аудиту без надмірного контролю з боку держави;

– введення штатних посад керівників та фахівців з кібербезпеки в державних органах, а також на об'єктах критичної інфраструктури.» [83]

Кабінет Міністрів України до 20.07.2025 р. має забезпечити прийняття нормативно-правових актів, необхідних для реалізації Закону України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури», привести у відповідність з ним свої нормативно-правові акти і нормативно-правові акти міністерств та інших центральних органів виконавчої влади.

1.1.3 Закон України «Про критичну інфраструктуру»

Закон України «Про критичну інфраструктуру» [96] був введений в дію з 15.06.2022 р. (остання редакція від 21.09.2024 р.).

Закон України «Про критичну інфраструктуру» регулює процеси функціонування та захисту КІ та об'єктів критичної інфраструктури (ОКІ) у мирний час. Питання забезпечення кіберзахисту об'єктів критичної інформаційної інфраструктури (ОКІІ) регулюються окремими нормативно-правовими актами. Також іншими законами регулюються процеси функціонування та захисту КІ та ОКІ в умовах надзвичайного та воєнного стану, надзвичайних ситуацій та особливого періоду. До таких законів відносяться Закон України «Про оборону України», закони «Про правовий режим воєнного стану» і «Про правовий режим надзвичайного стану», «Про функціонування єдиної транспортної системи України в особливий період» та інші.

В Законі України «Про критичну інфраструктуру» визначені ряд базових термінів, засади державної політики у сфері захисту КІ і організаційні засади національної системи захисту КІ, структура і принципи керування КІ та національною системою захисту КІ.

Державна політика захисту КІ спрямована на забезпечення безпеки штатного функціонування ОКІ, унеможливлення несанкціонованого втручання в процеси їх функціонування і захисту шляхом моніторингу стану безпеки, прогнозування, розробки та впровадження ефективних і своєчасних заходів запобігання кризовим ситуаціям на ОКІ та заходів щодо пом'якшення наслідків реалізації загроз ОКІ та ОКІІ ОКІ.

Суб'єктами національної системи захисту КІ є уповноважений орган у сфері захисту КІ України; центральний орган виконавчої влади, який забезпечує формування та реалізує державну політику у сфері цивільного захисту; секторальні та функціональні органи, інші міністерства та центральні органи виконавчої влади. Зокрема, суб'єктами національної системи захисту КІ є Кабінет Міністрів України; Національний банк України; Служба безпеки України; Апарат Ради національної

безпеки і оборони України; Збройні Сили України; Адміністрація Державної служби спеціального зв'язку та захисту інформації України (ДССЗЗІ); Центральна виборча комісія; Фонд державного майна України; Національні комісії з цінних паперів та фондового ринку, державного регулювання у сфері зв'язку та інформатизації, державного регулювання у сферах енергетики та комунальних послуг; правоохоронні та розвідувальні органи; місцеві органи виконавчої влади; військово-цивільні адміністрації; органи місцевого самоврядування; суб'єкти оперативно-розшукової та контррозвідувальної діяльності; оператори КІ; підприємства, установи та організації, які (незалежно від форми власності) забезпечують безпеку та стійкості КІ.

Національна система захисту КІ має декілька рівнів управління (загальнодержавний, регіональний та галузевий, місцевий та об'єктовий), для кожного з яких визначені відповідальні за її функціонування органи:

–загальнодержавний рівень: Кабінет Міністрів України -, уповноважений орган у сфері захисту КІ України; Національний банк України; органи державної влади; центральні органи виконавчої влади; інші державні органи;

–регіональний та галузевий рівні: центральні та місцеві органи виконавчої влади, що є відповідальними за формування та реалізацію державної політики у сфері захисту КІ в окремому секторі КІ або за функціонування окремих державних систем захисту та реагування;

–місцевий рівень: місцеві органи виконавчої влади; військово-цивільні адміністрації; органи місцевого самоврядування в межах своїх повноважень;

–об'єктовий рівень: оператор КІ.

Закон виокремлює серед органів управління ті органи, що визначають порядок віднесення об'єктів до КІ для банківського сектору і сфери, яка регулюється державними органами. Відповідні об'єкти також розглядаються окремо.

При оцінюванні належності об'єкта до КІ використовується визначена в Законі сукупність критеріїв, що дозволяють оцінити значимість об'єкта для забезпечення національної, соціальної, політичної, економічної та, екологічної

безпеки; для реалізації життєво важливих функцій та надання життєво важливих послуг громадянам України. Критерії оцінювання поділяються на секторальні і міжсекторальні.

Перелік секторів і підсекторів КІ, суб'єктів, що відповідають за їх безпеку, та відповідних життєво важливих функцій та послуг, які надаються в секторах і підсекторах, визначається Кабінетом Міністрів України.

Законом «Про критичну інфраструктуру» [96] визначено як життєво важливі ряд функцій і послуг, серед яких - транспортне забезпечення.

За законом «Про критичну інфраструктуру» КІ може функціонувати в чотирьох режимах, які оголошуються секторальними органами захисту КІ:

– у штатному режимі;

– у режимі готовності та запобігання реалізації загроз;

– у режимі реагування на виникнення кризової ситуації;

– у режимі відновлення штатного функціонування

Згідно із Законом, за секторальними і міжсекторальними критеріями визначається категорія критичності ОКІ. Категоризація ОКІ проводиться окремо в кожному секторі або підсекторі секторальними органами. При категоризації всі об'єкти інфраструктури певного сектору поділяються на чотири категорії (I – особливо важливі об'єкти, II - життєво важливі об'єкти, III – важливі об'єкти, IV – необхідні об'єкти).

Після категоризації на кожен ОКІ складається Паспорт безпеки, вимоги до змісту якого визначені Законом «Про критичну інфраструктуру» [96]. В Паспорті наводиться інформація щодо ідентифікації об'єкта, інформація про заходи безпеки, інформація про осіб, які є відповідальними за присвоєну категорію і за зв'язок та обмін інформацією з суб'єктами національної системи захисту КІ. Паспорти безпеки для ОКІ розробляються операторами основних послуг і безкоштовно погоджуються секторальними органами, незалежно від форми власності ОКІ.

Суб'єкти національної системи захисту КІ можуть вносити пропозиції щодо врахування життєво важливих функцій та послуг і структури національної системи захисту КІ.

В Україні ведеться загальнодержавний Реєстр об'єктів КІ, інформація до якого вноситься за пропозиціями суб’єктів національної системи захисту КІ і за звітами у визначеному форматі, які оформлюють секторальні органи шляхом об’єднання інформації про ОКІ всіх підсекторів даного сектору.

Багато статей Закону присвячені організації співробітництва на різних рівнях управління міжнародних організацій, державних органів, органів місцевої влади і самоврядування, приватного сектору та інших суб’єктів національної системи захисту КІ.

1.2 Властивості інформації, що забезпечуються КСЗІ

1.2.1 Властивості інформації, що враховуються при побудові системи захисту за стандартним функціональним профілем захищеності

В НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу» [64] і в НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» [65] приймаються до уваги чотири властивості захищеності інформації – конфіденційність (англ. *Confidentiality*), цілісність (англ. *Integrity*), доступність (англ. *Availability*) і спостереженість (англ. *observability*), тобто застосовується модель загроз *CIAO*.

Залежно від класу автоматизованої системи і необхідності забезпечувати вищезгадані властивості інформації в НД ТЗІ 2.5-005-99 [65] можна обрати стандартний функціональний профіль захищеності, за яким за допомогою НД ТЗІ 2.5-004-99 [64] визначаються вимоги до комплексу засобів захисту (КЗЗ) щодо виконуваних ним функцій і процедур його розробки та впровадження. В тому числі визначаються вимоги до документаційного супроводу цих процесів (як частина вимог гарантій коректності реалізації КЗЗ).

1.2.2 Властивості інформації, що враховуються при побудові системи захисту за базовим профілем безпеки інформації

При побудові системи безпеки інформації (СБІ) за базовим профілем безпеки згідно з НД ТЗІ 2.6-004-21 [66], НД ТЗІ 3.6-004-21 [67], НД ТЗІ 3.6-005-21 [68], НД ТЗІ 3.6-006-21 [69], НД ТЗІ 3.6-007-21 [70], НД ТЗІ 3.6-008-21 [71], НД ТЗІ 3.7-003-2023 [72] рішення щодо типу СБІ для конкретної інформаційно-комунікаційної системи (ІКС) приймається в залежності від типу ІКС та характеристик інформації (рис.1.1), що циркулює в ІКС.

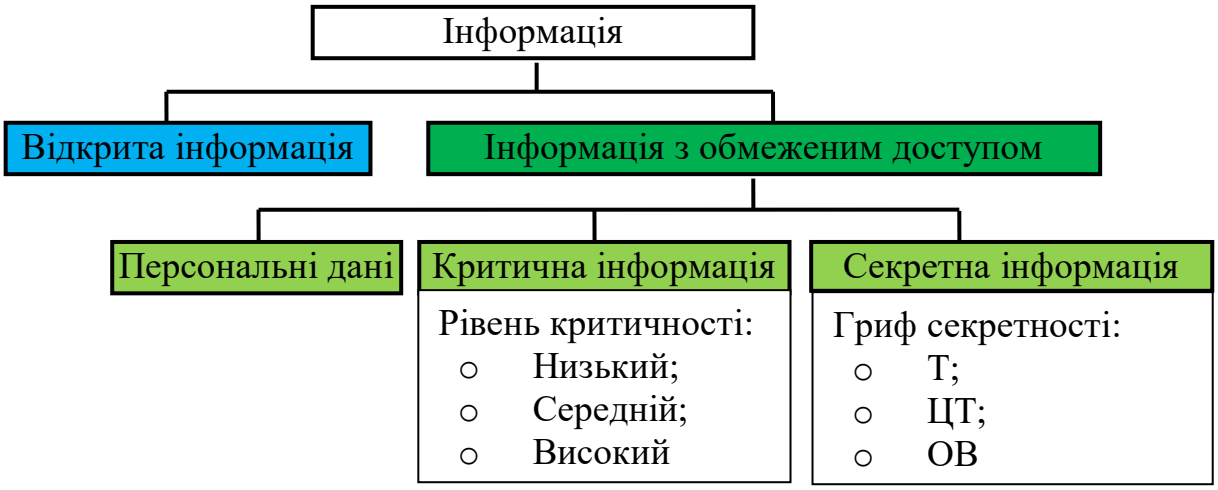


Рисунок 1.1 – Характеристики інформації в ІКС

КСЗІ і СБІ створюється для того, щоб забезпечити:

– конфіденційність інформації – унеможливити отримання інформації неавторизованим користувачем;

– цілісність інформації – унеможливити модифікацію інформації неавторизованим користувачем;

– доступність інформації – забезпечити авторизованим користувачам час очікування доступу до визначених політикою безпеки інформаційних ресурсів і сервісів не більше заданого;

– спостережність інформації – забезпечити можливість відстежувати і фіксувати суб’єктів та їх однозначну ідентифікацію для розслідувань порушень політики безпеки.

СБІ мають задовольняти:

−вимогам безпеки, які можуть походити з різних джерел (нормативно-правова бази, політика безпеки організації) і є визначеннями потреб у безпеці інформації (активів) з врахуванням супутніх обмежень та умов;

−вимогам приватності, які випливають із законодавчо визначених засад захисту персональних даних і дозволів осіб на використання даних, за якими їх можна однозначно ідентифікувати.

СБІ мають забезпечувати цифрові ідентичності і для відкритої інформації - збереження цілісності та доступності, а для інформації з обмеженим доступом (ІзОД) - збереження конфіденційності, тобто доступ до неї лише авторизованими цифровими ідентичностями.

За змістом інформації розрізняють при цьому:

−цифрову ідентичність - інформацію про сутність для представлення сутності зовнішнім агентам (фізичним особам, організаціям, за стосункам, пристроям);

−персональні дані – інформацію про фізичну особу, за якою ця особа може бути однозначно ідентифікована;

−критичну інформацію – ІзОД без ознак державної таємниці, порушення властивостей захищеності якої (порушення конфіденційності, цілісності, доступності) може мати негативні наслідки для власника інформації та/або ІКС, у якій вона циркулює. Критична інформація розрізняється за рівнем критичності (низький, середній, високий) за тяжкістю наслідків порушення її властивостей захищеності (порушень конфіденційності, цілісності, доступності). До критичної інформації також належать службова інформація, комерційна таємниця, банківська таємниця та інщі види таємниць, що захищаються державою;

−секретна інформація (інформація з грифом секретності) - інформація, розголошення якої може завдати шкоди національній безпеці України. Секретна інформація (інформація, яка згідно діючого законодавства має ознаки державної таємниці) розрізняється за грифами секретності (Т – таємно, ЦТ –

цілком таємно, ОВ – особливої важливості). Для доступу для такої інформації користувачі повинні мати відповідні форми допуску.

Рівень критичності інформації характеризує інформацію та ІКС за тяжкістю можливих негативних наслідків порушення конфіденційності, цілісності або доступності інформації в певній ІКС для суспільства, держави, організацій, особи:

– інформація і ІКС з високою категорією критичності - негативні наслідки для діяльності організації є суттєвими, ІКС та/або організація втрачає здатність виконувати свої функції за призначенням;

– інформація і ІКС з середньою категорією критичності - негативні наслідки для діяльності організації є помірними, ІКС та/або організація втрачає здатність виконувати хоча б одну зі своїх функцій за призначенням або виконує їх із суттєвим зниженням ефективності;

– інформація і ІКС з низькою категорією критичності негативні наслідки для діяльності організації є незначними, ІС та/або організація зберігають здатність виконувати свої функції за призначенням із незначним зниженням ефективності або здатні викоувати ці функції із залученням доступних додаткових ресурсів і засобів.

Характеристики інформації, за якими вона відноситься до державної таємниці визначаються Законом України «Про державну таємницю» [87].

Служба безпеки України (СБУ) формує і підтримує в актуальному стані Звід відомостей, що становлять державну таємницю [50]. Зокрема, державну таємницю становлять відомості про організацію системи оборони територій, про матеріальне і кадрове забезпечення (наявність, заплановані поставки, розташування тощо) військових підрозділів і органів правопорядку, заплановані закупівлі товарів оборонного призначення, скрите управління військами тощо.

В морській галузі державну таємницю становлять відомості про:

– кількість, типи, марки, запас ходу підйомно-транспортної техніки, морських і річкових суден, місце розташування портових споруд і територій, що вилучаються для забезпечення мобілізаційного розгортання військ;

−зміст заходів маскування дійсних параметрів рівнів фізичних полів корабля і організаційно-технічні заходи, що необхідні для контролю або компенсації цих рівнів;

−результати науково-дослідних і дослідно-конструкторських робіт, пов'язаних військовою технікою;

−опис, схеми, автоматизовані системи життєзабезпечення, технічні засобів охорони, порядок і плани експлуатації спеціальних споруд.

Гриф секретності інформаційних ресурсів встановлюється і змінюється залежно від обсягу і важливості наявних в них і визначених Зводом відомостей.

1.3 Загальна характеристика нормативно-правової бази кібербезпеки у галузі водного транспорту

Серед Законів України можна виділити закони, які стосуються кіберзахисту взагалі, закони щодо захисту критичної інфраструктури, закони щодо транспорту і водного транспорту (рис.1.2). Причому в останній групі законів питання кібербезпеки не розглядаються (хіба що опосередковано – наприклад як передумова безпеки судноплавства, але якоїсь конкретики в них не має). Крім того, є закони, які діють у мирний час і втрачають чинність, тобто замінюються іншими законами при певних умовах (наприклад - в разі надзвичайного чи воєнного стану, в особливий період).

Як показав проведений аналіз, нормативно-правова база дослідження за змістом має складну структуру (рис.1.3) і включає в себе блоки нормативно-правових актів, що на державному рівні стосуються:

−управління якістю товарів і послуг;

−захисту критичної інфраструктури (закони України «Про критичну інфраструктуру» [96], «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» [84]);

Рисунок 1.2 – Закони України у галузі водного транспорту

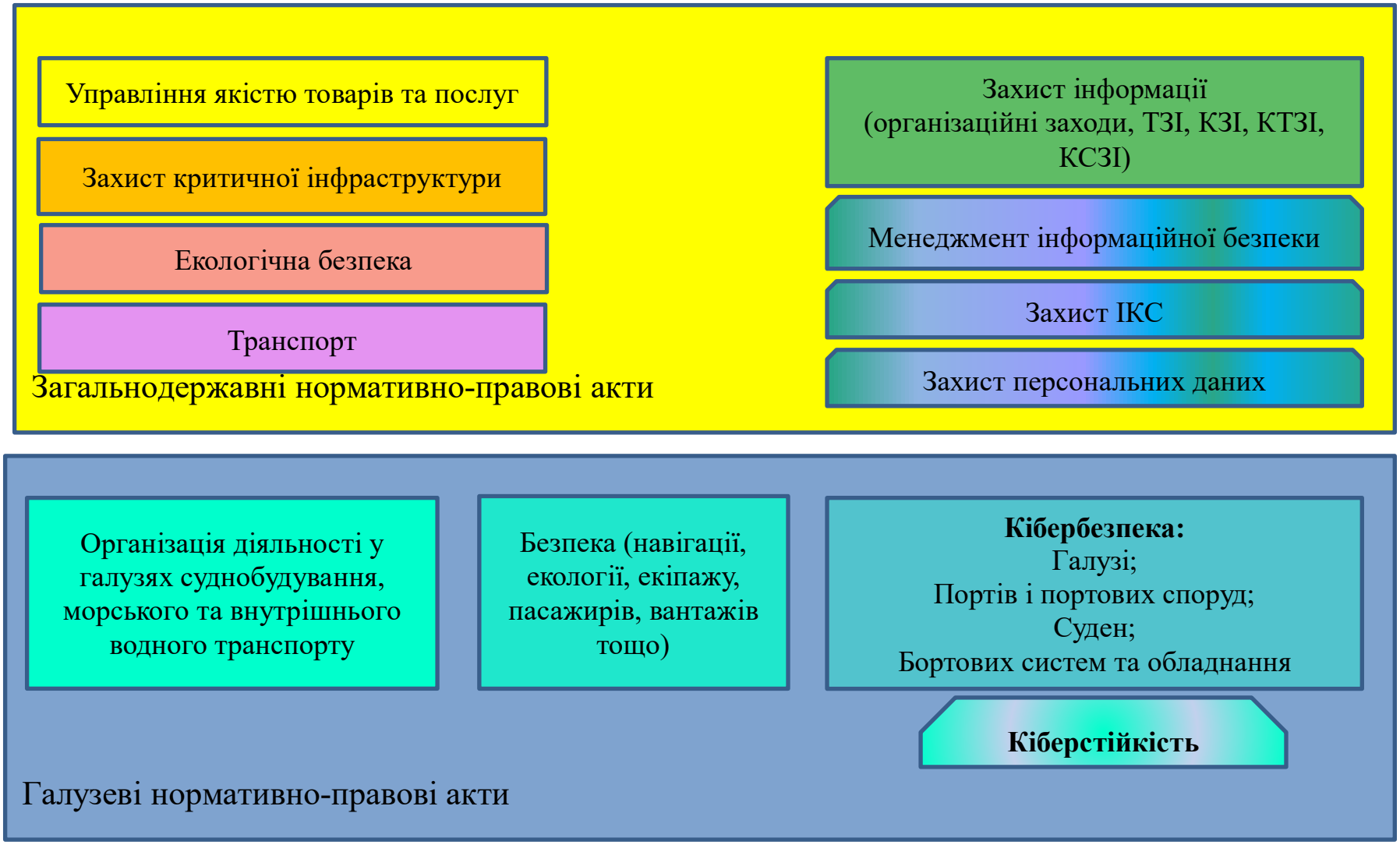


Рисунок 1.3 – Структура нормативно-правової бази

−екологічної безпеки;

−організації транспортних систем (закони України «Про транспорт», «Про внутрішній водний транспорт»);

−захисту інформації (організаційного, технічного і криптографічного), питань розробки комплексів технічного захисту інформації і комплексних систем захисту інформації. Велика група документів стосується питань менеджменту інформаційної безпеки, захисту персональних даних, захисту інформаційно-комунікаційних систем.

Серед нормативно-правових актів загальнодержавного рівня також слід відзначити Стратегію кібербезпеки України, друга редакція якої була затверджена Указом Президента України у 2021 році [101] і плани її реалізації [76, 89], які затверджуються постановами Кабінету Міністрів України як органом виконавчої влади.

На галузевому рівні можна виділити нормативно-правові акти щодо:

−організації діяльності у галузі водного транспорту;

−різних аспектів безпеки у галузі водного транспорту, зокрема питань безпеки (безпеки навігації, безпеки перевезення пасажирів і вантажів, екологічної безпеки, безпеки екіпажу тощо) в тому числі – питань кібербезпеки.

Серед нормативно-правових актів, які стосуються кібербезпеки, можна виділити документи, які регламентують питання кібербезпеки портів, суден, суднового обладнання і бортових систем, морської галузі в цілому, а серед них, окремо - документи, що стосуються кіберстійкості.

1.4 Нормативно-правові акти на рівні міністерств

До нормативно-правової бази дослідження також входять Укази Президента України; Постанови, Рішення і Розпорядження Кабінету Міністрів України, Ради національної безпеки і оборони тощо.

Наприклад:

– Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»» [101];

– Розпорядження Кабінету Міністрів України №430-р від 30.05. 2018 р. «Про схвалення Національної транспортної стратегії України на період до 2030 року» [98];

– Розпорядження Кабінету Міністрів України №1163-р від 19 грудня 2023 р. «Про затвердження плану заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України» [89].

Серед Постанов Кабінету Міністрів України можна виділити:

а) постанови, що стосуються організації діяльності в галузі захисту інформації:

– №373 від 29.03.2006 р., що затвердила «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» [82];

– №411 від 3.09.2014 р., що затвердила «Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України» [77];

– №609 від 5.08.2015 р., що затвердила перелік органів ліцензування в галузі інформаційної безпеки;

– №93 від 11.02.2016 р., що затвердила бланки ліцензії єдиного зразка для певних видів господарської діяльності;

– №821 16.11.2016 р., що затвердила перелік послуг, що підлягають ліцензуванню у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації, ліцензійні умови провадження цієї господарської діяльності, рекомендований перелік засобів вимірювальної техніки та контролю і обладнання, необхідних для надання послуг у галузі технічного захисту інформації, що підлягають ліцензуванню [22];

– №1295 від 23.12.2020 р., що затвердила «Порядок функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки» [81];

– №1426 від 29.12.2021 р., що затвердила «Положення про організаційно-технічну модель кіберзахисту» [79];

б) постанови, що стосуються захисту критичної інфраструктури:

– №518 від 19.06.2019 р., що затвердила «Загальні вимоги до кіберзахисту об'єктів КІ» [49];

– №943 від 9.10.2020 р., що затвердила «Порядок внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування» і «Порядок формування переліку об'єктів критичної інформаційної інфраструктури»[23];

– №1109 від 9.10.2020 р., що затвердила «Перелік секторів (підсекторів), основних послуг КІ держави», «Порядок віднесення об'єктів до об'єктів КІ», «Методику категоризації об'єктів КІ, затверджена Постановою Кабінету міністрів України» [24];

– №821 від 22.07.2022 р., що затвердила «Порядок проведення моніторингу рівня безпеки об'єктів критичної інфраструктури» [91];

– №48 від 16.01.2024 р., згідно з якою у Постанову Кабінету Міністрів України від 9 жовтня 2020 р. №1109 були внесені зміни, зокрема, суттєво розширився «Перелік секторів (підсекторів), основних послуг КІ держави» [86];

в) постанови, що стосуються організації діяльності в морській галузі:

– №136 від 9.02.2022 р., що затвердила «Перелік внутрішніх морських вод і внутрішніх водних шляхів, віднесених до категорії судноплавних» [88].

Постанови Правління Національного Банку України регулюють питання кібербезпеки у сфері відповідальності Національного Банку України і фактично стосуються всіх стейкхолдерів у морській галузі України:

– №4 від 16.01.2021, що затвердила «Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг»;

–№ 43 від 19.05.21, що затвердила «Положення про захист інформації та кіберзахист учасниками платіжного ринку»;

–№ 172 від 20.12.23, що затвердила «Положення про використання електронного підпису та електронної печатки»;

–№ 49 від 14.04.23, що затвердила «Положення про використання засобів криптографічного захисту інформації Національного банку України».

До 2021 року стосовно кібербезпеки було видано Наказ Міністерства фінансів України № 466 від 20.07.04, яким були затверджені «Правила доступу до приміщень, в яких розмішене серверне та комунікаційне обладнання» і «Рекомендації з технічного захисту інформації в приміщеннях серверних, електронної пошти та інших спеціальних приміщень».

Наказом Міністерства транспорту України №904 від 20.11.2003 було затверджене «Положення про систему управління безпекою судноплавства на морському і річковому транспорті» [80], яке не розглядає питання кібербезпеки окремо, але необхідність захисту інформації логічно випливає із задач забезпечення екологічної безпеки, безпеки навігації, пасажирів, вантажів тощо.

Питань інформаційної безпеки та кібербезпеки, безпеки водного транспорту як сектора критичної інфраструктури, питань розробки, впровадження і перевірки ефективності КСЗІ стосуються такі накази Адміністрації Держспецзв’язку як:

− №45 від 26.03.2007, яким затверджено «Порядок оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації» [59];

− №93 від 16.05.2007, яким затверджено «Положення про державну експертизу у сфері технічного захисту інформації» [78];

− №23 від 15.01.2021, яким затверджено «Методичні рекомендації щодо категоризації об'єктів КІ» [56];

− №899 від 18.10.2023, яким затверджено «Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб» [90];

– №354 від 10.07.2024 [92], яким затверджено «Рекомендації з оцінки достатності заходів захисту інформації комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації» [100];

– №317 від 24.06.2024 [57], яким визначено базові профілі безпеки інформації для ІКС, де обробляється відкрита інформація, і для ІКС, де обробляється службова інформація;

– №531 від 26.09.2024 про внесення змін до НД ТЗІ 2.3-025-21.

Центральним управлінням Служби безпеки України були видані накази:

№1519/533 від 04.09.2018 (сумісний наказ з Адміністрацією ДССЗЗІ), яким затверджено нормативний документ «Технічні засоби для здійснення уповноваженими органами оперативно-розшукових заходів та негласних слідчих (розшукових) дій у телекомунікаційних мережах загального користування України. Загальні технічні вимоги»;

– №1132 від 22.07.2019, яким затверджено «Порядок проведення державної експертизи комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах Служби безпеки України»;

– №383 від 23.12.2020, яким затверджено «Звід відомостей, що становлять державну таємницю» [61], що регулярно оновлюється;

– №627/772 від 19.12.2024 (сумісний наказ з Адміністрацією ДССЗЗІ) «Деякі питання розробки, затвердження та погодження планів захисту об’єктів критичної інфраструктури за проектною загрозою національного рівня «кібератака/ кіберінциденти» [58].

Міністерства оборони України 17.10.2023 видало Наказ №605 «Про затвердження Переліку відомостей Міністерства оборони України, які містять службову інформацію (ПСІ-2023)» [60], що доповнює «Звід відомостей, що становлять державну таємницю» [61].

Крім того, при розробці КСЗІ слід використовувати «Перелік засобів криптографічного захисту інформації, які мають експертний висновок за

результатами державної експертизи у галузі КЗІ» [74] і «Перелік засобів ТЗІ, які мають експертний висновок про відповідність вимогам технічного захисту інформації» [75].

1.5 Міжнародні нормативно-правові акти

1.5.1 Директиви і Регламенти Європейського союзу

Серед міжнародних нормативно - правових актів, слід в першу чергу виділити Конвенцію про кіберзлочинність [54], яка визначає принципи спільної протидії кіберзлочинності країн-учасниць. Крім того, є ряд конвенцій стосовно безпеки в морській галузі:

– Міжнародна конвенція з охорони людського життя на морі;

– Міжнародна конвенція про запобігання забрудненню з суден;

– Міжнародна конвенція про пошук і рятування на морі.

Група європейських Директив і регламентів стосується захисту критичної інфраструктури:

2004 рік: формулювання вимоги щодо розробки загальної стратегії захисту КІ; ухвалення Європейською комісією «Повідомлення про охорону та захист КІ», в якому захист КІ розглядався в контексті боротьби з тероризмом і були запропоновані можливі заходи Співтовариства для запобігання, підготовки та реагування на терористичні атаки, що стосуються КІ;

2005 рік: Європейська комісія затвердила Зелену книгу щодо європейської програми захисту та охорони КІ, обговорення якої виявило нагальну потребу у вдосконаленні захисту КІ в Європі та зменшення її вразливості, переваги спільних дій у межах Співтовариства щодо безпеки КІ кожної країни і Європи в цілому. У грудні 2005 року збула сформульована пропозиція розробити Європейську програму захисту КІ (англ. *European Programme for Critical Infrastructure Protection, EPCIP*), яка б охоплювала всі типи загроз (техногенні, технологічні та природні) та пріоритетно протидіяла

терористичним атакам. В результаті в *EPCIP* були встановлені принципи та інструменти, необхідні для реалізації *EPCIP*, спрямованої як на європейську, так і на національну інфраструктуру.

2007 рік: Рада Європи затвердила висновки щодо програми *EPCIP* [2], наголосивши, що країни-члени несуть повну відповідальність за управління механізмами захисту КІ на національному рівні. Заходи, спрямовані на сприяння впровадженню *EPCIP*, включали в себе:

− план дій *EPCIP*;

− створення інформаційної мережі попередження про критичну інфраструктуру (англ. *Critical Infrastructure Warning Information Network, CIWIN*);

− створення груп експертів із захисту КІ на рівні ЄС;

− регламентування процесів обміну інформацією щодо захисту КІ, ідентифікації та аналізу взаємозалежностей;

− підтримку країн ЄС щодо національних критичних інфраструктур (англ. *National Critical Infrastructures, NCI*), які за бажанням можуть використовуватися певною країною ЄС;

− планування на випадок надзвичайних ситуацій;

− супутні заходи фінансової підтримки, зокрема, Спеціальну програму ЄС «Запобігання, підготовка та управління наслідками тероризму та інших ризиків, пов'язаних з безпекою» на період 2007-2013 роки, яка забезпечила фінансування заходів, пов'язаних з *CIP*.

2008 рік: видана Директива Ради 2008/114/ЄС «Про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту» [95], яка стала першим кроком до ідентифікації та визначення європейських критичних інфраструктур (ЄКІ) і розробки методик оцінювання їх захисту. Основна увага в Директиві [95] була зосереджена на енергетичному і транспортному секторах, проте зазначалося, що наявна потреба у подальшій роботі й поширенні дії Директиви на інші сектори, зокрема на сектор інформаційно-комунікаційних технологій (ІКТ). В

Директиві [95] зазначається, що внаслідок наявності взаємозалежності і взаємних зв'язків інфраструктур різних країн, пошкодження або знищення певних *NCI* може мати істотні транскордонні наслідки. Такі КІ необхідно ідентифікувати та визначати як ЄКІ за єдиною процедури для всіх країн ЄС. Заходи із забезпечення захисту ЄКІ є масштабними і не можуть бути самостійно проведені окремою державою-членом із достатньою ефективністю, тобто цілі Директиви 2008/114/ЄС недосяжні на рівні держави-члена, однак досяжні на рівні Співтовариства. Як критерії для ідентифікації ЄКІ Директива 2008/114/ЄС визначила потенційні наслідки порушень її штатного функціонування для окремих осіб, економіки, екології та соціуму.

2016 рік: прийнята Директива Європейського Парламенту та Ради (ЄС) 2016/1148 «Про заходи високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу» [94], в якій вказувалося, що для європейської співпраці у питаннях кіберкриз потрібно створити Групу співпраці, до складу якої увійдуть представники держав-членів, Європейської комісії та Європейського агентства з мережевої та інформаційної безпеки (англ. *European Union Agency for Network and Information Security, ENISA*), мережа груп реагування на інциденти з комп'ютерною безпекою (англ. *Computer Emergency Response Team, CSIRT*), що складатиметься з національних *CSIRT* держав-членів і *CSIRT* ЄС. Директива (ЄС) 2016/1148 розглядала три типи цифрових послуг (послуга хмарних обчислень, електронний торговий майданчик; електронна пошукова система), виокремлювала вже сім секторів КІ, і визначила операторів основних послуг в мережевих та інформаційних системах кожного підсектору. Зокрема у підсекторі «Водний транспорт» сектору «Транспорт» як оператори основних послуг були визначені оператори служб руху суден; керівні органи портів; суб'єкти, які експлуатують установки та обладнання, розташовані в портах; компанії, що є операторами морського, внутрішнього, каботажного, пасажирського та вантажного водного транспорту. Оператори основних послуг та надавачі цифрових послуг відповідають за забезпечення безпеки мережевих та інформаційних систем, які вони

використовують, незалежно від того хто здійснює технічне обслуговування цих систем (сам оператор чи стороння організація), а виробники апаратного забезпечення та розробники програмного забезпечення є відповідальними за свої товари, хоча вони не є операторами основних послуг чи надавачами цифрових послуг. При розголошенні інцидентів слід забезпечувати баланс між потенційною шкодою репутації чи бізнесу операторів основних послуг та надавачів цифрових послуг, які повідомляють про інциденти компетентні органи, та інтересами громадськості щодо сповіщень про загрози. Держава-член ЄС не зобов'язана надавати інформацію, розкриття якої суперечить, на її думку, суттєвим інтересам її безпеки. Виконуючи зобов'язання щодо оприлюднення інформації про загрози, *CSIRT* та компетентні органи повинні зберігати конфіденційність інформації про вразливості продукту доти, поки не будуть видані відповідні виправлення безпеки і рекомендації щодо їх застосування. У підсекторі «Водний транспорту» вимоги безпеки висуваються до всіх операцій, у тому числі – до систем радіо- та електрозв'язку, комп'ютерних систем та мереж компаній, кораблів та служб руху суден, портів і портових споруд. Визначення операторів у підсекторі водного транспорту має бути, узгодженим між державами-членами, тому держави-члени при визначені операторів в цьому підсекторі повинні враховувати існуючі та розроблювані міжнародні кодекси та настанови, зокрема, документи Міжнародної морської організації. Директива (ЄС) 2016/1148, відома як Директива *NIS* (англ. *Network and Information Security Directive*), діяла до січня 2023 року і втратила чинність у зв'язку із введенням Директиви (ЄС) 2022/2555 [1].

2022 рік: прийняття Директиви (ЄС) 2022/2555 [1], відомої як відома як *NIS*2, яка набула чинності з 16 січня 2023 року. Необхідність заміни Директиви (ЄС) 2016/1148 на *NIS*2 зумовлена розширенням спектрів секторів КІ, ОКІ та ОКІІ. Національне законодавство держав-членів ЄС мало бути приведене у відповідність до *NIS*2 до жовтня 2024 року. Вимоги Директиви (ЄС) 2022/2555 переважно орієнтовані на середні і великі компанії, однак, уряди можуть

зобов'язати виконувати вимоги цієї директиви й невеликі компанії, що мають високий ступінь ризиків безпеки. *NIS*2 [1] передбачає:

– збільшення кількості секторів КІ;

– виокремлення серед інфраструктур основних (ключових, англ. *essential*) та важливих (англ. *important*), а серед організацій - *essential*-компаній та *important*-компаній. *Essential*-компаніями є організації, функціонування яких є критично важливим для виконання державою своїх функцій і/або для життя та здоров'я громадян. Поняття *essential*–інфрастуктура значно співпадає з поняттям КІ, а *essential*-компанія – з поняттям ОКІ;

– виокремлення 11 *essential*-секторів в інфраструктурі держави (зокрема, «Транспортування», «Цифрова інфраструктура», «Управління послугами ІКТ») та 7 *important*-секторів (серед яких «Постачальники цифрових послуг» - платформи соціальних мереж онлайн-ринки та пошукові системи);

– усування різниці між постачальниками цифрових послуг і операторами критичних чи важливих послуг;

– обов'язкові ключові заходи технічного та організаційного захисту (як мінімум), які повинні впровадити усі *essential* та *important* суб'єкти, серед яких: розробка і впровадження політики безпеки ІКС із визначеними процедурами аналізу ризиків, врегулювання інцидентів, антикризового менеджменту, управління резервним копіюванням, застосування шифрування та криптографічних засобів захисту; впровадження практик кібергігієни, зокрема, надійної багатофакторної автентифікації;

– поділ інцидентів на суттєві і несуттєві. Суттєвим є інцидент, який може призвести відносно суб'єкта господарювання до значних оперативних збоїв у наданні послуг чи великих фінансових і/або нематеріальних збитків, може суттєво вплинути на інших фізичних чи юридичних осіб;

– диференціацію процедур звітування про інциденти залежно від того, чи є інцидент суттєвим. Не дозволяється суб'єктам, що потрапляють під дію *NIS*2, приховувати інформацію про суттєві інциденти. Контролери даних мають інформувати суб'єктів даних про певні порушення даних згідно вимог

прийнятого у 2016 році Загального регламенту захисту даних (англ.. *General Data Protection Regulation, GDPR*);

– обов'язкове надсилання суб'єктом, що потрапляє під дію *NIS*2, до *CSIR*T держави-члена ЄС або до відповідного наглядового органу повідомлення про будь-який суттєвий інцидент протягом 24 годин, попередній звіт про інцидент - протягом 72 годин, остаточний звіт - не пізніше ніж через місяць. Остаточний звіт має містити детальні описи інциденту, його першопричини, типу загрози, наслідків (зокрема - транскордонного впливу), заходів, які вживалися для пом'якшення наслідків та запобігання появі інцидента в майбутньому;

– обов'язкове надсилання суб'єктом, що потрапляє під дію *NIS*2 і надає послуги, повідомлення одержувачам цих послуг про суттєві інциденти, які можуть негативно вплинути на надання цих послуг, та про заходи правового захисту, які можуть застосувати одержувачі послуг у відповідь на загрозу збоїв у постачанні послуг;

– надавач послуг повинен усувати ризики у своєму ланцюзі поставок, а отримувачі товарів і послуг – враховувати ризики в ланцюгах поставок;

– покладання на держав-членів ЄС обов'язків забезпечення ефективного контролю компетентними органами стану безпеки;

– уніфікація процедур правозастосування в рамках ЄС. В усіх державах-членах ЄС діють однакові вимоги до звітності органів контролю за станом безпеки, які органи застосовують однакові процедури контролю (такі як інспекції на місцях, цільові аудити безпеки) і мають однакові права (право запитувати інформацію і вимагати докази виконання політики кібербезпеки, право отримувати доступ до даних); а також застосовуються при однакових правопорушення однакові міри покарання (позбавлення сертифікату чи ліцензії, заборона керівнику організації або законному представнику виконувати певні обов'язки, накладання штрафів на *essential*-організації до 10 мільйонів євро/ 2 % річного світового обороту і на *important*-організації до 7 мільйонів євро /1,4 % річного світового обороту);

– використання міждержавної структури, що має сприяти безпеці європейського кіберпростору - мережі зв'язку організацій з європейських кіберкриз (англ. *European Cyber Crisis Liaison Organization Network, EU-CyCLONe*). *EU- CyCLONe* була запущена у 2020 році та офіційно оформлена 16 січня 2023 року з набранням чинності *NIS*2. Метою *EU- CyCLONe* є організація співпраці, своєчасного обмін інформацією та підвищення ситуаційної обізнаності держав-членів ЄС за допомогою інструментів *ENISA.* Основними завданнями *EU CyCLONe* є: підвищення рівня готовності держав членів і Євросоюзу в цілому до управління масштабними кіберінцидентами, координація управління великими кіберризиками на оперативному рівні, оцінювання наслідків масштабних інцидентів у сфері кібербезпеки, розробка і оприлюднення можливих заходів пом'якшення наслідків кіберінцидентів, в тому числі – організація на запит держави-члена обговорення національних масштабних кіберінцидентів та планів реагування на кризи;

– використання для кожного сектору підготовлених *ENISA* роз'яснень [13], в яких зазначені: ключові виклики кібербезпеці в даному секторі; сфера дії *NIS*2 в даному секторі; зміни, пов'язані з *NIS*2 для даного сектора включено до контролю; термін, до якого сектор має бути приведений у відповідність *NIS*2.

Таким чином, місцева влада має здійснювати активний моніторинг безпеки ключових (*essential*) підприємств і організацій, а центральні органи підключаються до управління, якщо є докази інциденту. *Essential* та важливі *important* компанії мають бути безпечними, забезпечувати безпеку свого ланцюжка поставок, звітувати про стан безпеки і чітко повідомляти про те, як вони реагують на кіберінциденти.

У липні 2019 року Організація економічного співробітництва та розвитку (англ. *Organisation for Economic Co-operation and Development, OECD* - міжнародна організація, що об'єднує 38 країн світу, серед яких більшість європейських країн, США, Австралія та інші країни з розвиненою економікою) опублікувала звіт про КІ своїх членів і найліпші практики забезпечення стійкості

критичних інфраструктур «*Good Governance for Critical Infrastructure Resilience*» [9], у якому були виявлені розбіжності у принципах визначенні КІ різних країн:

– визначення національних секторів, виходячи з міркувань важливості захисту економічного та соціального добробуту;

– визначення національних секторів, виходячи переважно з міркувань важливості національної безпеки;

– комбінований підхід, що об'єднує два попередніх і застосовується, наприклад, у Великобританії.

Кількість секторів КІ і їх склад також різняться для різних країн (наприклад, США має 16 секторів КІ, Великобританія - 13, Австралія – 8, Бразилія – 5) внаслідок того, що кожна країна має власну інфраструктуру і по-своєму визначає національні пріоритети обробки ризиків безпеки. Кількість секторів КІ у кожній країні з часом змінюється. Наприклад, в США у 1996 році було вісім секторів КІ, у 1998 році – 15, у 2001 році 9, у 2019 році – 16 секторів КІ.

В усіх державах, що є членами *OECD*, застосовується підхід спільної відповідальності до забезпечення безпеки КІ. Такий підхід на даний час вважається найкращою практикою. Згідно цього підходу:

– національні КІ і КІІ мають бути ідентифіковані;

– має бути прийнята національна стратегія кібербезпеки, в якій визначені керівні принципи управління безпекою та координації спільних зусиль з її забезпечення;

– мають бути створені координаційні органи із забезпечення безпеки;

– уряди несуть відповідальність за безпеку КІ та КІІ і через координаційні органи управляють процесами ідентифікації КІ та КІІ та управляють процесами захисту КІІ за принципами, визначеними у національній стратегії кібербезпеки;

– в процесах ідентифікації КІ та КІІ приймають активну участь державні та приватні оператори КІ та КІІ, а також інші ключові зацікавлені сторони;

– зазвичай застосовується наступний порядок ідентифікації КІ та КІІ: спочатку визначаються сектори і основні послуги КІ, а потім - сектори і послуги КІІ. Деякі країни дотримуються іншого порядку.

Для України міжнародне співробітництво у сфері захисту КІ і кібербезпеки, зокрема, співробітництво з ЄС, є стратегічним завданням. Першочерговою задачею для виконання цього завдання є гармонізація нормативно-правових актів, що вимагає уніфікації процедур ідентифікації КІ, КІІ, ОКІ та ОКІІ, а також процедур оцінювання критичності ОКІ та ОКІІ.

Оскільки базовий профіль безпеки має задовольняти вимогам приватності, то серед міжнародних нормативно-правових актів слід зазначити:

– Директиву 95/46/ЄС Європейського Парламенту і Ради "Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних" від 24 жовтня 1995 року [25];

– Директиву 97/66/ЄС Європейського Парламенту і Ради «Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі» від 15 грудня 1997 року [26];

– Директиву №2002/58/ЄС Європейського Парламенту і Ради ЄС стосовно обробки персональних даних та захисту права на недоторканість особистого життя в сфері електронних комунікацій (Директива про право на недоторканість особистого життя та комунікації, електронні засоби зв'язку) [27];

– Конвенцію про захист прав людини і основоположних свобод. [53];

– Конвенцію про захист осіб у зв'язку з автоматизованою обробкою персональних даних [52].

1.5.2 Міжнародні і вітчизняні стандарти

Серед міжнародних стандартів слід виділити низку стандартів, виданих Міжнародною організацією зі стандартизації (англ. *International Organization for Standardization, ISO*) і Міжнародною електротехнічною комісією (англ. *International Electrotechnical Commission, IEC*), які стосуються управління інформаційною безпекою, вимог приватності і екології. Більшість цих

міжнародних стандартів у модифікованому або ідентичному вигляді імплементовані в Україні як державні стандарти (табл.1.1).

Таблиця 1.1 – Міжнародні і вітчизняні стандарти

№	Міжнародні стандарти	ДСТУ
1	-	ДСТУ 2226-93 «Автоматизовані системи. Терміни та визначення» [28]
2	-	ДСТУ 3396.0-96 «Захист інформації. Технічний захист інформації. Основні положення» [29]
3	-	ДСТУ 3396 1-96 «Захист інформації. Технічний захист інформації. Порядок проведення робіт» [30]
4	-	ДСТУ 3396.2-97 «Захист інформації. Технічний захист інформації. Терміни та визначення» [31]
5	*ISO* 7498-2-89 *Information proceeding systems. Open Systems Interconnection. Basic Reference Model. Part 2: Security Architecture* [7]	-
6	*ISO/IEC* 9001:2015 «*Quality management systems. Requirements*»	ДСТУ *ISO* 9001:2015 Системи управління якістю. Вимоги (*ISO/IEC* 9001:2015, *IDT*) [36]
7	*ISO/IEC* 14001:2015 «*Environmental management systems. Requirements with guidance for use*»	ДСТУ *ISO* 14001:2015 Системи екологічного управління. Вимоги та настанови щодо застосовування (ISO 14001:2015, IDT) [37]
8	*ISO/IEC* 15408-1:2022 «*Information security, cybersecurity and privacy protection — Evaluation criteria for IT security. Part* 1: *Introduction and general model*»	ДСТУ *EN ISO/IEC* 15408-1:2022 Інформаційні технології. Методи захисту. Критерії оцінювання. Частина 1. Вступ та загальна модель (*EN ISO/IEC* 15408-1:2020, *IDT; ISO/IE*C 15408-1:2009, *IDT*) [33]
9	*ISO/IEC* 15408-2:2008 «*Information security, cybersecurity and privacy protection — Evaluation criteria for IT security. – Part* 2: *Security functional components*»	ДСТУ *EN ISO/IEC* 15408-2:2022 Інформаційні технології. Методи захисту. Критерії оцінювання. Частина 2. Функціональні вимоги (*EN ISO/IEC 15408-2:2020, IDT; ISO/IEC* 15408-2:2008, *IDT*) [34]
10	*ISO/IEC* 15408-3:2022 «*Information security, cybersecurity and privacy protection — Evaluation criteria for IT security. – Part* 3: *Security assurance components*»	ДСТУ *EN ISO/IEC* 15408-3:2022 Інформаційні технології. Методи захисту. Критерії оцінювання. Частина 3. Вимоги до гарантії безпеки (*EN ISO/IEC* 15408-3:2020, *IDT; ISO/IEC* 15408-3:2008, *IDT*) [35]
11	*ISO/IEC* 15408-4:2022 «*Information security, cybersecurity and privacy protection — Evaluation criteria for IT security. – Part* 4: *Framework for the specification of evaluation methods and activities*»	ДСТУ *ISO/IEC* 15408-4:2023 Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 4. Структура для визначення методів оцінювання та діяльності (*ISO/IEC* 15408-4:2022, *IDT*) [38]
12	*ISO/IEC* 15408-5:2022 «*Information security, cybersecurity and privacy protection — Evaluation criteria for IT security. – Part* 5: *Pre-defined packages of security requirements*»	ДСТУ *ISO/IEC* 15408-5:2023 Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 5. Попередньо визначені пакети вимог до безпеки (*ISO/IEC* 15408-5:2022, *IDT*) [39].

Продовження таблиці 1.1

№	Міжнародні стандарти	ДСТУ
13	*ISO/IEC* 17799:2005 «*Information technology. Security techniques. Code of practice for information security management*» [8]	-
14	*ISO/IEC* 18045:2022 «*Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation*»	ДСТУ *EN ISO/IEC* 18045:2022 Інформаційні технології. Методи захисту. Методологія оцінювання безпеки IT (*EN ISO/IEC* 18045:2020, *IDT; ISO/IEC* 18045:2008, IDT) [40]
15	*ISO/IEC* 27000:2018 «*Information technology — Security techniques — Information security management systems — Overview and vocabulary*»	ДСТУ *ISO/IEC* 27000:2019 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів (*ISO/IEC* 27000:2018, *IDT*) [41]
16	*ISO/IEC* 27001:22 «*Information security, cybersecurity and privacy protection — Information security management systems — Requirements*»	ДСТУ *ISO/IEC* 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (*ISO/IEC* 27001:2022, *IDT*) [42]
17	*ISO/IEC* 27002:2022 «*Information security, cybersecurity and privacy protection — Information security controls*»	ДСТУ *EN ISO/IEC* 27002:2024 Інформаційна безпека, кібербезпека та захист конфіденційності. Заходи забезпечення інформаційної безпеки (*EN ISO/IEC* 27002:2022, *IDT; ISO/IEC* 27002:2022, *IDT*) [43]
18	*ISO* 27005:2022 «*Information security, cybersecurity and privacy protection — Guidance on managing information security risks*»	ДСТУ *ISO/IEC* 27005:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки (*ISO/IEC* 27005:2022, *IDT*) [44]
19	*ISO/IEC* 27035-1:2023 «*Information technology — Information security incident management. Part* 1: *Principles and process*»	ДСТУ ISO/IEC 27035-1:2024 Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 1. Принципи та процес (*ISO/IEC* 27035-1:2023, *IDT*) [45]
20	*ISO/IEC* 29100:2024 «*Information technology – Security techniques – Privacy framework*»	ДСТУ 7731:2015 «Інформаційні технології. Методи захисту. Основні положення щодо забезпечення невтручання в особисте життя (*ISO/IEC* 29100:2011, *MOD*)» [32]
21	*ISO/IEC* 29101:2018 «*Information technology — Security techniques — Privacy architecture framework*»	ДСТУ *EN ISO/IEC* 29101:2022 Інформаційні технології. Методи захисту. Структура архітектури забезпечення прайвесі (*EN ISO/IEC* 29101:2021, *IDT; ISO/IEC* 29101:2018, *IDT*) [46]
22	*ISO* 31000:2018 «*Risk management — Guidelines*»	ДСТУ *ISO* 31000:2018 Менеджмент ризиків. Принципи та настанови (*ISO* 31000:2018, *IDT*) [47]
23	*IEC* 31010:2019 «*Risk management — Risk assessment techniques*»	ДСТУ *EN IEC* 31010:2022 Керування ризиками - методи оцінки ризиків (*EN IEC* 31010:2019, *IDT; IEC* 31010:2019, *IDT*) [48]

Крім ДСТУ при створенні системи захисту інформації часто необхідно враховувати будівельні норми і правила (наприклад, ДБН 2.2-3-2012 «Склад,

порядок розроблення, погодження та затвердження проектної документації для будівництва» [21]) та керівні документи (наприклад, РД 50-34.698-90 «Автоматизовані системи. Вимоги до змісту документів» [99]).

Також слід відзначити наявність ряду зарубіжних національних стандартів, які де-факто стали міжнародними стандартами. Так, наприклад, НД ТЗІ 3.6 -004-21 «Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці» [67] посилається на стандарти, випущені американським Національним інститутом стандартів і (англ. *United States National Institute of Standards and Technology's*, *NIST*), серед яких виокремлюються федеральні публікації щодо стандартів обробки інформації (англ. *Federal Information Processing Standards Publication*, *FIPS PUB*) [20]:

а) *FIPS PUB:*

− 199 *«Standards for Security Categorization of Federal Information and Information Systems»* (2004 р.);

− 200 *«Minimum Security Requirements for Federal Information and Information Systems»* (2006 р.);

б) «*NIST Framework for Improving Critical Infrastructure Cybersecurity* (*Cybersecurity Framework*)», *Version* 1.1 (2018 р.);

в) *NIST Special Publication*:

− 800-30. *Rev.*1. *«Guide for Conducting Risk Assessments»* (2012 р.);

− 800-37. *Rev.*2. *«Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy»* (2018 р.);

− 800-39. *«Managing Information Security Risk: Organization, Mission, and Information System View»* (2011);

− 800-53. *Rev.*5 *«Security and Privacy Controls for Information Systems and Organizations»* (2020 р.);

− 800-64. *Rev.*2. *«Security Considerations in the System Development Life Cycle»* (2008 р.);

− 800-128. *«Guide for Security-Focused Configuration Management of Information Systems»* (2011 р.);

− 800-160 *Vol.* 1. *«Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems»* (2018 р.);

− 800-160 *Vol.* 2. *«Developing Cyber Resilient Systems: A Systems Security Engineering Approach»* (2019 р.).

1.5.3 Рекомендації і вимоги з кібербезпеки провідних міжнародних організацій у галузі водного транспорту

У галузі водного транспорту діє низка великих міжнародних організацій, які самостійно або у складі групи видають рекомендації і вимоги щодо різноманітних аспектів безпеки, серед цих організацій слід виділити наступні:

− Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (англ. *European Union Agency for Network and Information Security, ENISA*);

− Агентство міжнародного розвитку США (англ. *United States Agency for International Development, USAID*);

− Асоціація будівельників супер’яхт (англ. *Superyacht Builders Association, Sybass*);

− Асоціація цифрових контейнерних перевезень (англ. *Digital Container Shipping Association, DCSA*);

− Балтійська і міжнародна морська рада (англ. *Baltic and International Maritime Council, BIMCO*);

− Всесвітня рада судноплавства (англ. *World Shipping Council, WSC*);

− Комітет з морської безпеки *IMO* (англ. *Maritime Safety Committee, MSC*);

− Міжнародна асоціація власників суховантажних суден (англ. *International Association of Dry Cargo Shipowners, INTERCARGO*);

− Міжнародна асоціація класифікаційних співтовариств (англ. *International Association of Classification Societies, IACS*);

− Міжнародна асоціація морських підрядників (англ. *International Marine Contractors Association, IMCA*);

− Міжнародна асоціація незалежних власників танкерів (англ. *International Association of Independent Tanker Owners, INTERTANKO*);

− Міжнародна асоціація портів та гаваней (англ. *International Association of Ports and Harbours, IAPH*);

− Міжнародна морська організація (англ. *International Maritime Organization, IMO*);

− Міжнародний морський форум нафтових компаній (англ. *Oil Companies International Marine Forum, OCIMF*);

− Міжнародна палата судноплавства (англ. *International Chamber of Shipping, ICS*);

− Міжнародний союз морського страхування (англ. *International Union of Marine Insurance, IUMI*);

− Організація економічного співробітництва та розвитку(англ. *Organisation for Economic Co-operation and Development, OECD*);

− Північний морський центр кіберстійкості (англ. *Nordic Maritime Cyber Resilience Centre, NORMA Cyber*);

− Судноплавна палата Америки (англ. *Chamber of Shipping of America, CSA*);

− Центр обміну та аналізу інформації та системи морського транспорт, США (англ. *Maritime Transportation System Information Sharing and Analysis Center, MTS-ISAC*).

Однією з найважливіших міжнародних угод з безпеки мореплавства є Міжнародна конвенція з охорони людського життя на морі *SOLAS* (англ. *International Convention for the Safety of Life at Sea*), метою якої є встановлення мінімальних стандартних вимог з безпеки при будівництві, обладнанні та експлуатації суден. Дія *SOLAS* не поширюється на військові кораблі і судна для

перевезення військ, малотонажні судна, рибальські судна, яхти, деревяні судна і судна без механічного приводу, на судна, які здійснюють перевезення виключно по Великих Озерах в Північній Америці і річці Святого Лаврентія.

SOLAS містить вимоги до:

– конструкції плавзасобів – вимоги до поділу на відсіки, остійність;

– рятувальних засобів – вимоги до шлюпок, плотів, мотоботів, рятувальних кругів і жилетів, розклад по тривогам;

– бортових систем – вимоги до механічного та електричного устаткування, засобів захисту від шуму, засобів протипожежного захисту, радіозв'язку, засоби зв'язку пожежників;

– засобів забезпечення безпеки мореплавання – вимоги до штормтрапів і систем тривожної сигналізації ходової вахти про льоди, шторми, катастрофи, пошуки тощо;

– умов перевезення вантажів – вимоги до перевезення рідкого палива, насипних вантажів (наприклад, зерна), небезпечних вантажів;

– безпечної експлуатації суден (англ. *International Safety Management* (*ISM*) *code, ISM code,* укр. Міжнародний кодекс з управління безпекою (МКУБ));

– заходів безпеки на високошвидкісних суднах, на навалювальних суднах, на ядерних суднах, на суднах, що експлуатуються в полярних водах;

– спеціальних заходів з підсилення охорони на морі (англ. *International Ship and Port Facility Security Code, ISPS code*, укр. Міжнародний кодекс охорони суден і портових засобів, Кодекс ОСПЗ) і з підвищення безпеки на морі;

IMO визначені критерії перевірки відповідності вимогам *SOLAS*, система і методи перевірки. МКУБ визначає правила проведення аудитів СУБ суден, і отримання ними відповідних сертифікатів. Кодекс ОСПЗ визначає правила взаємодії Договірних урядів, державних установ місцевих адміністрацій, представників СК і портів в процесах виявлення загроз, що стосуються охорони портів і суден, задіяних у міжнародних перевезеннях.

Договірні уряди мають право інспектувати судна, що ходять під прапорами інших держав, коли є підстави вважати, що судно або його

обладнання істотно не відповідають *SOLAS*. Процедура перевірки відповідності суден вимогам *SOLAS* отримала назву «державний портовий контроль». Якщо судно, що здійснює міжнародний рейс, не відповідає вимогам *SOLAS* з об'єктивних причин, то на нього має бути оформлене Вилучення за згодою Морської адміністрації прапора судна. В іншому випадку після перевірки судно може бути затримане, а в окремих випадках навіть не допущене в порт.

ISPS code містить функціональні вимоги до:

– збирання і оцінювання інформації, яка стосується загроз ОСПЗ;

– обміну інформацією, яка стосується загроз ОСПЗ, між Договірними Урядами, між суднами, між суднами і портовими засобами (зокрема щодо дотримання протоколів зв'язку для суден і портових засобів) та іншими береговими об’єктами;

– заходів запобігання несанкціонованому допуску на судна, портові засоби й на їх райони обмеженого доступу членів екіпажів суден, пасажирів і відвідувачів, робітників порту;

– запобігання доставці на судна або на портові засоби недозволених предметів: вибухових речовин, запальних пристроїв, недозволеної зброї тощо;

– підготовки персоналу, проведення занять і навчань з метою ознайомлення із планами охорони і здобуття практичних навичок реагування на інциденти охорони та надзвичайні ситуації;

– засобів тривожної сигналізації про загрози або інциденти ОСПЗ

– наявності і змісту планів ОСПЗ, що базуються на оцінках охорони.

За ОСПЗ відповідають:

– офіцери охорони суден, які призначаються компанією і є підзвітними капітану;

– офіцер охорони компанії, який призначається компанією і відповідає за проведення оцінки охорони судна; розробку, впровадження і підтримку плану охорони судна; зв'язок з офіцерами охорони портових засобів та офіцером охорони судна. Відомості про офіцера охорони компанії, зокрема інформація для цілодобового зв'язку з ним заносяться у план охорони судна;

– офіцери охорони портових засобів, які призначаються в портах відповідальними за розробку, впровадження, перегляд і виконання планів охорони портових засобів і за зв'язок з офіцерами охорони суден та офіцерами охорони компаній.

Охорона може підтримуватися заходами охорони на 3-х рівнях:

– рівень охорони 1 - постійно підтримуються мінімальні заходи з охорони;

– рівень охорони 2 - протягом певного періоду через підвищену небезпеку інциденту з охорони підтримуються спеціальні додаткові заходи з охорони;

– рівень охорони 3 - протягом обмеженого періоду, коли інцидент охорони є ймовірним або неминучим, хоча ціль нападу може бути й невідомою, підтримуються підвищені спеціальні заходи з охорони.

Рівні охорони встановлюються Договірними Урядами, врахуванням:

– ступеня довіри до інформації про загрозу;

– ступеня підтвердження інформації стосовно загрози;

– ступеня невідворотності і конкретизації загрози;

– тяжкості можливих наслідків інциденту, пов'язаного з охороною.

ISPS code встановлює правила обміну інформацією щодо рівнів охорони для офіцерів охорони, Адміністрацій і Договірних Урядів

В плані охорони судна міститься інформація, яка є ІзОД, зокрема, інформація щодо суднових систем тривожного сповіщення (з метою уникнення перешкоджанню досягненню цілі її встановлення) і розташування постів приведення їх в дію може зберігатися на судні в іншому місці, у документі, відомому капітану, офіцеру охорони судна та іншому старшому персоналу на судні, на розсуд Компанії.

Резолюція *MSC.428(98)* 2017 «*Maritime cyber risk management in safety management systems*» [11] (укр. «Управління морськими кіберризиками в системах управління безпекою») і *MSC-FAL.1/Circ.3* «*Guidelines on maritime cyber risk management*» (укр. «Настанови щодо управління морськими кіберризиками») випущені *MSC* 2017 році.

MSC.428 (98) 2017 [11] визнає нагальну необхідність усунути кіберзагрози та вразливі місця в морській галузі, оскільки кібертехнології стали важливими для функціонування та управління численними системами, що є критично важливими для безпеки, зокрема, для безпеки судноплавства та захисту морського середовища. Цей документ визначає, що затверджені за вимогами *ISM code* системи управління безпекою (СУБ) повинні враховувати управління кіберризиками, Власники і оператори суден повинні оцінювати кіберризики та впроваджувати відповідні заходи в усіх функціях їхньої СУБ до першого Документа про відповідність після 1 січня 2021 року. *MSC.*428 (98) також визнає необхідність збереження конфіденційності певної інформації про кіберризики.

MSC-FAL.1/Circ.3 надає загальні методичні вказівки щодо проведення оцінки кіберризиків для дотримання резолюції *MSC.*428(98). Друга редакція *MSC-FAL.1/Circ.3/Rev.2* [12] вийшла 17 червня 2022 року. *MSC-FAL.1/Circ.3* вимагає, щоб зацікавлені сторони вжити необхідні заходи для захисту судноплавства від поточних і нових загроз і вразливостей, пов’язаних із оцифровуванням, інтеграцією та автоматизацією процесів і систем у судноплавстві.

Кібертехнології стали важливими для роботи та управління численними системами, критично важливими для безпеки та безпеки судноплавства та захисту морського середовища. У деяких випадках ці системи повинні відповідати міжнародним стандартам і вимогам Адміністрації прапорів. Однак вразливі місця, створені в результаті доступу до цих систем, їх взаємозв’язку чи об’єднання в мережу, можуть призвести до кіберризиків, які слід усунути. Вразливі системи можуть включати, зокрема: системи мостів; системи обробки та управління вантажем; системи керування силовими установками та механізмами; системи керування живлення; системи контролю доступу; системи обслуговування та управління пасажирами; мережі загального користування, орієнтовані на пасажирів; адміністративні та соціально-побутові системи екіпажу; системи зв'язку.

При організації кіберзахисту необхідно враховувати різницю між інформаційними технологічними (IT) системами та операційними технологічними системами (OT-системами):

– IT-системи використовують дані як інформацію, що підлягає обробці, збереженню, аналізу тощо;

– OT-системи використовують дані для моніторингу або управління фізичними процесами.

Крім того, при побудові СУБ слід також розглянути захист інформації та обмін даними в IT та OT системах. Ризики в IT і OT системах можуть бути наслідком уразливості, що виникає через неадекватну роботу, інтеграцію, технічне обслуговування та проектування кібер-складових IT і OT систем, а також через навмисні та ненавмисні кіберзагрози. Загрози виявляють або використовують вразливі місця (наприклад, ПЗ чи неефективні брандмауери) в операційній чи інформаційній технології. Ефективне управління кіберризиками має враховувати обидва типи загроз, вразливості у IT-системах, які можуть виникнути внаслідок неправильного підключення до робочих технологічних систем або процедурних помилок оперативного персоналу чи третіх осіб (наприклад, неналежне використання знімних носіїв, таких як карта пам’яті).

Під час розгляду потенційних джерел загроз і вразливостей, а також пов’язаних із цим стратегій зменшення ризиків слід також брати до уваги ряд потенційних варіантів засобів контролю для управління кіберризиками, включаючи, серед іншого, організаційне, операційне або процедурне і технічне управління.

Метою управління морськими кіберризиками є підтримка безпечного та захищеного судноплавства, яке є експлуатаційно стійким до кіберризиків.

Управління кіберризиками означає процес виявлення, аналізу, оцінки та повідомлення про кіберризик, а також прийняття, уникнення, перенесення або пом’якшення його до прийнятного рівня, враховуючи витрати та переваги дій, вжитих для зацікавлених сторін. Ефективне управління кіберризиками підтримують 5 функціональних складових, які включені в структуру управління ризиками і мають діяти не послідовно, а одночасно і неперервно: ідентифікація, захист, виявлення кібер-подій, реагування на кібер-події (планування), відновлення після інцидентів.

Для отримання детальної інформації та вказівок, пов’язаних із розробкою та впровадженням конкретних процесів управління ризиками, користувачі *MSC-FAL.1/Circ.3* повинні звернутися до конкретних вимог Договірних урядів і Адміністрацій прапорів, а також до відповідних міжнародних і галузевих стандартів і найкращих практик. *MSC-FAL.1/Circ.3* рекомендує:

– «*The Guidelines on Cyber Security Onboard Ships*» [17], розроблені великою групою організацій і провідних компаній морської галузі (див.п.1.2.1 даної кваліфікаційної роботи) щодо кібербезпеки на борту суден;

– консолідовану рекомендацію *IACS* щодо кіберстійкості в морській галузі «*Recommendation on Cyber Resilience*» *No*. 166 (*Rec 166*) [16];

– міжнародний стандарт *ISO/IEC* 27001 (остання версія - *ISO/IEC 27001:2022 «Information security, cybersecurity and privacy protection — Information security management systems — Requirements*») щодо управління інформаційною безпекою (в Україні ДСТУ *ISO/IEC* 27001:2023 [42]);

– фреймворк *NIST* - концепцію *NIST* щодо покращення кібербезпеки КІ;

– «*IAPH Cybersecurity Guidelines for Ports and Port Facilities*» [6] - рекомендації *IAPH* щодо кібербезпеки для портів і портових засобів.

Оскільки в галузі судноплавства немає двох однакових організацій, то *MSC-FAL.1/Circ.3* [12] спеціально виражені в широких термінах, щоб мати широку сферу застосування, тобто є узагальненими рекомендаціями. Судна з обмеженими кіберсистемами можуть вважати достатнім просте застосування цих узагальнених рекомендацій, проте судна зі складними кіберсистемами можуть вимагати вищого рівня деталізації ризиків, і їм доведеться шукати і використовувати додаткові інформаційні ресурси - робочі посібники із кібербезпеки галузі, судна, порту, бортових комп’ютерних систем і обладнання з покроковими інструкціями і рекомендаціями найкращих практичних рішень щодо ефективного виявлення загроз, реагування на них і відновлення у разі кібератаки. При цьому управління кіберризиками за вимогами *IMO* має бути інтегроване в існуючі СУБ відповідно до Кодексу *ISM* і Кодексу *ISPS*.

Уніфіковані вимоги Міжнародної асоціації класифікаційних товариств до комп'ютерних систем *IACS UR E*22 «*Computer-based systems*» (прийняті у 2006 році., остання редакція – червень 2023 року [3]) є обов'язковими для нових суден з 1 червня 2024 року. Областю застосування *IACS UR E*22 є весь життєвий цикл комп'ютеризованих систем управління, сигналізації, моніторингу, забезпечення безпеки і внутрішнього зв'язку судна, але не застосовуються до навігаційних систем і радіо-комунікаційних систем (регулюються главами V і IV *SOLAS*). В *IACS UR E*22 визначені умови віднесення комп'ютеризованих систем до I, II і III категорії критичності. Уніфіковані вимоги до комп'ютерних систем поділяються на 5 груп:

1) загальні вимоги: на протязі життєвого циклу системи мають застосовуватися стандарти, вказані в *IACS UR E*22, або стандарти, визнані класифікаційним товариством, і має бути впроваджена система управління якістю відповідно до *ISO* 9001 та *IEC/ISO* 90003, для якої в *IACS UR E*22 визначені 15 обов'язкових вимог для систем II і III категорії;

2) вимоги до складових системи: наявність плану управління якістю для систем II і III категорії, однозначна ідентифікація систем і програмного забезпечення, наявність описів систем, мережі і збоїв, сертифікована відповідність компонентів обладнання екологічним вимогам, вимоги до тестування програмного забезпечення, обладнання і систем в цілому;.

3) вимоги до системного інтегратора (яким зазвичай є верф): визначення і дотримання плану управління якістю; використання систем із визначеними категоріями; документування архітектури систем на судні; визначення порядку тестувань систем на борту судна як окремих одиниць, так і у інтегрованому варіанті;

4) вимоги до обслуговування комп'ютеризованих систем: вимоги до власника, системного інтегратора, постачальників;

5) вимоги до управління змінами;

6) технічні вимоги до комп'ютеризованих систем:

а) звітність щодо ідентифікації системи і її складових (автоматизоване журналювання), документування збоїв;

б) для систем II і III категорії: втрата окремих невзаємопов'язаних повідомлень не повинна спричинити втрату функціональності; будь-яка втрата функціональності має бути ліквідована місцевими/ ручними засобами; мають бути наявні засоби захисту комунікацій від перевантаження і засоби само тестування; має бути система тривожних сповіщень;

в) специфічні вимоги до бездротових мереж. Системи категорії III не повинні використовувати бездротовий зв’язок, а інші можуть його використовувати за ряду умов:

–мають бути застосовані визнані міжнародні протоколи, які забезпечують: надання одержувачу повідомлення інформації про цілісність даних; надання дозволу на підключення тільки з пристроїв, що входять в проект системи; шифрування конфіденційних і критичних даних; безпеку управління; захист мережевих активів; запобігання несанкціонованому доступу до мережевих активів;

–внутрішні бездротові системи в межах судна мають відповідати вимогам щодо діапазонів частот і потужностей сигналів Міжнародного союзу електрозв’язку та держави прапора;

–враховуються державні і місцеві правила порту щодо обмежень діапазонів частот і потужностей сигналів при бездротовій передачі;

–для бездротових систем передавання даних мають бути проведені випробування з тестуванням узгодження обладнання гавань - море, щоб продемонструвати, що радіочастотна передача не викликає збою будь-якого обладнання та не призводить до його відмов у результаті впливу електромагнітних перешкод під час очікуваних робочих умов;

г) перевірка відповідності технічним вимогам Класифікаційного товариства.

Рекомендації щодо кіберстійкості *IACS* «*Recommendation on Cyber Resilience No.* 166 (*Rec.* №166)» [16] були розроблені в рамках міжгалузевої співпраці у 2020

році *IACS* на підтримку розроблених нею раніше уніфікованих вимог *IACS UR E*26 «Кіберстійкість суден» [4] та резолюції *IMO* «Управління морськими кіберризиками в системах управління безпекою» *MSC*.428(98) [11] разом із *MSC-FAL.1/Circ.3/Rev.2* [12]. У випадку розбіжностей між *IACS UR E*26 [4] і *Rec.* №166 [16] перевагу мають *IACS UR E*26. Метою *Rec.* №166 є забезпечення всіх стейкхолдерів технічною інформацією для організації постачання стійких до кіберзагроз суден, стійкість яких можна підтримувати протягом усього терміну служби. Рекомендації [16] стосуються суднових мереж, які використовують цифровий зв'язок для з'єднання суднових систем між собою і для доступу до обладнання або мереж за межами судна.

Функціональні вимоги, сформульовані в [16] класифікуються відповідно до п'яти підцілей (ідентифікувати, захистити, виявляти, реагувати та відновлювати) та припущень щодо оперативних аспектів та аспектів управління, вказаних у додатку А Рекомендацій [16]. Методологію перевірки прийнятих рішень як частину підходу на основі цілей наведено в розділі 8 для різних етапів (перевірка проекту, випробування на борту після встановлення та протягом терміну експлуатації судна). Оскільки бортові мережі можуть взаємодіяти з мережами інших суден і берегом, то в [16] передбачені наступні процедури:

− сегментація мережі на різні зони відповідно до визначеного рівня ризику. Критичні системи повинні бути згруповані і розділені по зонах відповідно до рівня ризику, порядку керування ризикамиа, бажаного цільового рівня безпеки для кожної зони;

− визначення демілітаризованих зон, щоб забезпечити додаткові можливості зниження ризику між мережею з низьким цільовий рівень безпеки та мережею, яка виконує контрольні функції і має високий цільовий рівень безпеки, і мінімізувати кількість людей, які мають прямий доступ до пристроїв критичної зони контролю.

В *Rec.* №166 визначені рекомендовані способи сегментації для бортових мереж II і III категорій критичності, і визначені заходи захисту бортових мереж і для взаємодії між мережами, головним чином – від несанкціонованого

дистанційного доступу. Коректність реалізації дистанційної форми доступу має бути перевірена шляхом тестування, програму якого розробляє і виконує постачальник послуг або системний інтегратор.

Загальною метою кіберзахисту є забезпечення конфіденційності, цілісності та доступності даних. Залежно від призначення системи задачі забезпечення конфіденційності, цілісності та доступності даних можуть мати різний пріоритет. Наприклад, для ОТ-систем, які передають критично важливі для безпеки дані, пріоритет забезпечення доступності даних є вищим за пріоритет задачі забезпечення цілісності даних.

Наслідки неавторизованої модифікації, пошкодження даних або втрати даних можуть відрізнятися між даними ІТ-систем (зазвичай операційні дані з впливом на бізнес) і даними ОТ-систем (можуть включати контрольні точки для керування обладнанням і безпеки з впливом на безпеку або навколишнє середовище), де передача даних і оновлення реалізовані за допомогою мережі. Однак, цілі забезпечення безпеки даних в обох типах систем мають спільні риси і повинні розглядатися для системи в цілому.

Передбачається, що після апробації на реальних проектах і, можливо, доопрацювання *Rec.* №166 будуть використовуватися в якості уніфікованих вимог щодо кібервідмовостійкості.

«*Guidelines on Cyber Security Onboard Ships*» [17] (укр. Настанови з кібербезпеки на борту суден) були затверджені у квітні 2022 року і повинні однаково впроваджуватися товариствами *IACS* на суднах, які за контрактом будуються з 1 січня 2024 року або пізніше, та може використовуватися для інших суден як необов’язкова інструкція. Метою рекомендацій [17] є покращення безпеки екіпажу, навколишнього середовища, вантажів та суден.

Згідно [17] управління кіберризиками має бути невід’ємною частиною культури безпеки та безпеки компанії, впроваджуватися на різних рівнях компанії, в тому числі на березі і на борту. Деякі аспекти управління кіберризиками можуть включати комерційно чутливу або конфіденційну

інформацію, яка, за можливості, має виключатися із повідомлень, що передаються мережею.

Рекомендації [17] визначають як зацікавлену сторону агента, що є представником власника судна та/або фрахтувальника (принципала) у порту і неперервно взаємодіє із судновласниками, операторами, терміналами, постачальниками портових послуг та органами державного портового контролю шляхом обміну чутливою для судна інформацією, фінансовою інформацією та інформацією щодо координації дій в портах. Стандарти якості для агентів важливі, тому що, як і будь-який інший бізнес, агенти також можуть бути мішенню кіберзлочинців, наприклад, у зв'язку з доставкою IT або OT обладнання на судно, електронним шахрайством, фальшивими призначеннями суден програмами-вимагачамиі і зломом захисту. Помякшення наслідків кіберризиків можливе тільки при умові наявності спільної стратегії дій судновласників і агентів і їх узгодженій взаємодії.

Цифрові системи, що використовуються для завантаження, вивантаження, управління і контролю вантажів, в тому числі небезпечних вантажів, можуть мати інтерфейс з різноманітними береговими службами, включаючи порти, морські термінали та стивідорів. Такі системи можуть включати інструменти відстеження відправлення вантажів та їх пересування, які доступні вантажовідправникам через Інтернет і, відповідно, є вразливими до кіберзагроз.

Відвідування суден сторонніми особами, що вимагає підключення до одного чи кількох комп'ютерів на борту, також впливає на комунікації судна і берега. Відвідувачами судна в порту можуть бути продавці, портові та інший чиновники, представники морського терміналу, агенти, лоцмани та інші технічні працівники для посадки на судно та підключення пристроїв, зокрема, ноутбуків та планшетів. Деяким технічним працівникам може знадобитися використання знімних носіїв для оновлювання систем бортових комп'ютерів, завантаження даних та/або виконання інших завдань згідно з їх посадовими обов'язками. Розповсюдженою також є практика використання офіційними особами та офіцерами державного портового контролю бортових засобів для

«друку офіційних документів з наступним вимаганням скопіювати інформацію на невідомий змінний носій.

Іноді немає контролю над тим, хто має доступ до бортових систем, наприклад, під час сухого докування, простоїв або під час прийняття нового або відомого судна. У таких випадках важко визначити, чи є шкідливим програмне забезпечення, що залишилося в бортових системах. Рекомендується заборонити резервне копіювання даних, видалити конфіденційні дані на судні, можливо - перевстановити програмне забезпечення. Якщо це можливо, перед використанням системи слід сканувати на наявність шкідливих програм. Правильність функціонування ОТ-систем має бути перевірена до їх використання.

Уніфіковані вимоги Міжнародної асоціації класифікаційних співтовариств *IACS UR E*26 «*Cyber resilience of ships*» [4] були прийняті у квітні 2022 року і враховують вимоги *IACS UR E*22 «*Computer-based systems*» [3], *IACS UR E*27 «*Cyber resilience of on-board systems and equipment*» [5] , *IACS «Recommendation on Cyber Resilience No.* 166» [16]. Область застосування *IACS UR E*26 охоплює:

а) ОТ-системи борту суден, тобто комп’ютеризовані системи, що використовують дані для управління або моніторингу фізичних процесів: привод; рульове управління; якірні і швартові системи; системи генерування і розподілу електроенергії; системи пожежної сигналізації і пожежогасіння; системи обробки вантажів, трюмної води, баласту; завантаження комп'ютерів; система управління опаленням і постачанням гарячої води; системи утилізації сміття; навігаційний системи; система моніторингу та контролю зрідженого природного газу; та інші ОТ-системи, порушення функціонування яких може спричинити додаткові ризики для операцій на судні;

б) будь-які Інтернет-протоколи на основі спілкування інтерфейсів від борту судна до інших систем у сфері дії *IACS UR E*26: системи управління пасажиропотоками і відвідувачами, системи їх обслуговування; мережі, орієнтовані на використання пасажирами; адміністративні мережі; системи

життєзабезпечення екіпажу; будь-які інші системи, підключені до ОТ-систем судна постійно або тимчасово (наприклад, під час технічного обслуговування).

*IACS UR E*26 містить ряд визначень, зокрема:

– поверхня атаки - набір усіх можливих точок, де неавторизований користувач може отримати доступ до системи та отримати дані. Поверхня атаки складається з поверхонь двох категорій: цифрової та фізичної;

– основна система - комп'ютерна система, що сприяє наданню послуг, необхідних для руху, керування та безпеки судна. Основні послуги включають «Первинні основні послуги» та «Вторинні основні послуги»: Первинні основні послуги — це ті служби, які мають бути в безперервній роботі, щоб підтримувати рух і рульове керування. Вторинно важливі послуги – це ті служби, які не обов'язково повинні працювати безперервно для підтримки силової установки та рульового управління, але є необхідними для підтримки безпеки судна.

– зона безпеки - сукупність підключених комп'ютеризованих систем у сфері застосування *UR E*26, які потребують однакової політики контролю доступу. Кожна зона складається з одного інтерфейсу або групи інтерфейсів, до яких застосовується політика контролю доступу;

Основною метою *UR E*26 є підтримка безпечного та захищеного судноплавства, яке є операційно стійким до кіберризиків, шляхом впровадження ефективної системи управління кіберризиками. Для цього у п'яти функціональних елементах (ідентифікація, захист, виявлення, реагування, відновлення) визначено підцілі щодо управління кіберризиками. Функціональні/технічні вимоги наведено для досягнення конкретних підцілей кожного функціонального елемента. Вимоги призначені для того, щоб забезпечити однакову реалізацію зацікавленими сторонами та зробити їх застосовними до всіх типів суден таким чином, щоб забезпечити прийнятний рівень стійкості та застосувати до всіх класифікованих плавзасобів незалежно від експлуатаційних ризиків і складності ОТ-систем. Для кожної вимоги наводиться обґрунтування, короткий опис дій, які необхідно виконати, і документація, яка має бути доступною,

на кожному етапі життя судна та у зацікавлених сторін, які беруть участь у такому етапі. Також наведено критерії оцінки ефективності та тестування.

Вимоги повинні виконуватися під відповідальність зацікавлених сторін, залучених до проектування, будівництва та експлуатації судна, серед яких виділяють наступних стейкхолдерів: судновласник/компанія, конструктор суден/суднобудівний завод; системний інтегратор (зазвичай – верф); постачальник - виробник або постачальник апаратних та/або програмних продуктів, системних компонентів або обладнання; класифікаційне товариство.

Оцінка ефективності та тестування спрямовані на перевірку ефективного впровадження заходів, прийнятих для виконання вимог *UR E*26, і в основному базуються на проектуванні, розробці, підтримці та реалізації Плану тестування. Плану тестування є основним інструментом, призначеним для підтримки, наземного тестування та перевірки кіберстійкості. Він охоплює різні фази життя судна і передбачає залучення різних зацікавлених сторін.

Уніфіковані вимоги Міжнародної асоціації класифікаційних співтовариств *IACS UR E*27 «*Cyber resilience of on-board systems and equipment*» [5] були прийняті у квітні 2022 року (остання версія – вересень 2023 року) і уточнюють уніфікований вимоги до кіберстійкості бортових систем та обладнання.

Необхідність прийняття *IACS UR E*27 [5] була зумовлена тим, що захист судноплавства від поточних і нових загроз має включати низку засобів захисту, які постійно розвиваються, що вимагатиме включення функцій безпеки в обладнання та системи на стадії проектування та виробництва. Тому виникла необхідність визначення загального набору мінімальних вимог до систем та обладнання, відповідність якому дозволила б стверджувати, що систем та обладнання є кіберстійкими. *IACS UR E*27 з 1 січня 2024 року мають однаково впроваджуватися товариствами *IACS* на всіх суднах, контракт на будівництво яких був укладений після цієї дати, а для інших суден *IACS UR E*27 можуть використовуватися для як необов’язкове керівництво.

Область застосування *IACS UR E*27 [5] охоплює різні типи суден, причому для одних типів суден вимоги *IACS UR E*27 є обов’язковими (наприклад, для

пасажирських суден, мобільні морських бурових установок потужністю 500 Гт і вище, вантажних і високошвидкісних суден вантажопідйомністю 500 Гт і більше тощо), а для інших – мають характер рекомендацій (наприклад, для військових та десантних кораблів, прогулянкових яхт, що не призначені для торгівлі, вантажних суден з валовою місткістю менше 500 Гт тощо). Вимоги щодо кібервідмовостійкості, наведені в розділі 4 *UR E*27, застосовуються до всіх систем, які входять до сфери дії *UR E*26, якщо не вказано протилежне. Додаткові вимоги, пов'язані з інтерфейсом із ненадійними мережами, застосовуються лише до систем, у яких передбачено таке підключення.

*IACS UR E*27 [5] не містять деяких вимог, тому на додаток до них застосовуються *UR E*10 (для екологічних показників апаратного забезпечення) і *UR E*22 [3] (для безпеки обладнання для функціональності програмного забезпечення). Стосовно комп'ютерних систем і кіберстійкості *IACS UR E*27 [5] посилається також на ряд додаткових документів *IACS*: *IACS UR E*22 [3], *IACS UR E*26 [4] , *Rec.*166 [16].

Класифікаційне товариство не заперечує проти застосування для навігаційних і радіо-комунікаційних систем замість вимог розділу 4 *UR E*27 вимог *IEC* 61162-460 або інших еквівалентних стандартів при умові дотримання вимог *IACS UR E*26 [4].

*IACS UR E*27 [5] містить ряд важливих визначень, зокрема:

– компенсаційний контрзахід - альтернативне рішення для контрзаходу, що має використовуватися у комплексі засобів захисту або на додаток до нього для задоволення однієї або кількох вимог безпеки;

– засоби контролю - засоби управління ризиками, включаючи політику, процедури, інструкції, практику або організаційні структури, які за своєю природою можуть бути адміністративними, технічними, управлінськими або правовими;

– глибинна оборони - стратегія ІБ, яка об'єднує людей, технології та оперативні можливості для встановлення змінних бар'єрів між кількома рівнями та місіями організації;

– прошивка - ПЗ, яке вбудоване в електронні пристрої і забезпечує керування, моніторинг і маніпулювання даними розроблених продуктів і систем. Зазвичай таке ПЗ є автономним і недоступним для маніпуляцій користувача;

– зміцнення - практика зменшення вразливості системи шляхом зменшення її поверхні атаки;

– наступальний кіберманевр - дії, які призводять до відмови, погіршення, порушення, знищення або маніпулювання ОТ або ІТ-системам.

Заходи безпеки для *essential* - систем не повинні негативно впливати на їх доступність. Реалізація заходів безпеки не повинна спричиняти втрату функцій безпеки самого захисту, управління, моніторингу або втрату інших важливих функцій, що може призвести до негативних наслідків для здоров'я людей, безпеки та навколишнього середовища. Система має бути сконструйована так, щоб дозволити судну продовжувати виконання критично важливих операцій у спосіб, який забезпечує конфіденційність, цілісність і доступність даних, необхідних для безпеки судна, його систем, персоналу та вантажу.

Компенсаційні контрзаходи повинні відповідати меті та суворості початкової заявленої вимоги з урахуванням стандартів, на які посилаються, а також відмінностей між кожною вимогою та пов'язаними пунктами в стандартах, і відповідати принципам, визначеним у розділі 3.1.3 «*Description of security capabilities*» *UR E*27.

1.6 Нормативні документи з технічного захисту інформації щодо створення КСЗІ

Серед великої кількості НД ТЗІ можна виділити документи, які стосуються апробованого протягом багатьох років підходу до створення КСЗІ на основі стандартних функціональних профілів захищеності, нормативні документи, що приймають за основу базовий профіль безпеки, і нормативні документи які регулюють процедуру створення КСЗІ у загальному вигляді

(рис.1.4), зокрема – створення служби захисту інформації, технічного завдання на КСЗІ і порядок проведення робіт.

В НД ТЗІ 3.7-003-23 «Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-комунікаційній системі» [72] наявні посилання на:

− НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу»;

− НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу»;

− НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі» [62];

− НД ТЗІ 1.6-003-2004 «Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації»;

− НД ТЗІ 2.3-025-21 «Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці» [63];

− НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» [64];

− НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» [65];

− НД ТЗІ 3.6-001-2000 «Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу»;

− НД ТЗІ 3.6-003-2016 «Порядок проведення робіт зі створення та атестації комплексів технічного захисту інформації» ДСК;

− НД ТЗІ 3.6-004-21 «Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці [67];

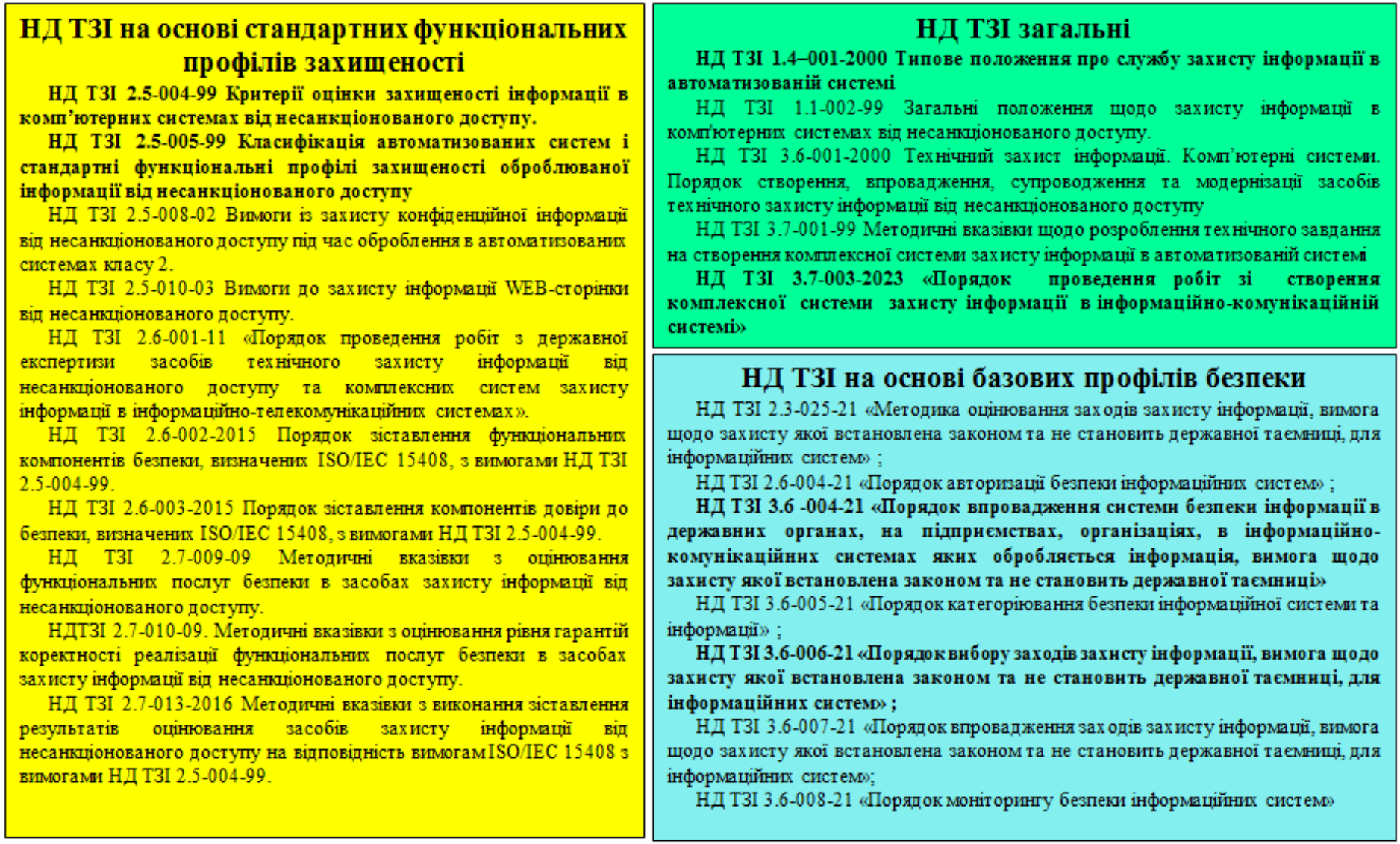


Рисунок 1.4 – Склад нормативних документів з технічного захисту інформації стосовно КСЗІ

− НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі».

− ДСТУ: ДСТУ 2226-93 [28], ДСТУ 3396.0-96 [29], ДСТУ 3396.1-96 [30], ДСТУ 3396.2-97 [31], ДСТУ 7731:2015 [32];

− ДБН: ДБН 2.2-3-2012 [21];

− РД 50-34.698-90 [99]

− *ISO*: *ISO* 7498-2-89 [7];

− Положення про державну експертизу у сфері технічного захисту інформації [78];

− Порядок оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації [59];

− Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб [90];

Таким чином, найбільші групи розглянутих нормативно-правових актів включають в себе десятки взаємопов’язаних документів.

Тому в даній роботі детальний аналіз проведено для трьох виділених на рис.1.4 НД ТЗІ і наказу Адміністрації Держспецзв’язку №317 24-го року, яким затверджено Базовий профіль безпеки.

2 АНАЛІЗ ДОКУМЕНТАЦІЙНОГО СУПРОВОДУ КСЗІ У ГАЛУЗІ ВОДНОГО ТРАНСПОРТУ

2.1 Модель впровадження системи безпеки інформації

Згідно з НД ТЗІ 3.7-003-23 «Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-комунікаційній системі» [72] роботи з побудови КСЗІ можуть проводитися з використанням базових профілів безпеки, затверджених Адміністрацією Держспецзв'язку, для відповідного виду інформації, що обробляється в ІКС.

Побудова КСЗІ ІКС з використанням базових профілів проводиться відповідно до НД ТЗІ 3.6-004-21 «Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці» [67]. Згідно з НД ТЗІ 3.6-004-21 модель впровадження системи безпеки інформації має вигляд рис.2.1 і передбачає, що незалежно від форми власності інформаційних систем (ІС):

– для інформаційних систем, які обробляють відкриту інформацію, мають розгортати СБІ, керуючись положеннями НД ТЗІ 3.6-004 [67] для впровадження відповідних заходів захисту, направлених на забезпечення цілісності та доступності відкритої інформації, яка циркулює у даних ІС.

– для ІС, які обробляють будь-які персональні дані мають розгортати СБІ керуючись положеннями НД ТЗІ 3.6 -004, а також вимог ДСТУ 7731:2015 «Інформаційні технологій. Методи захисту. Основні положення щодо забезпечення невтручання в особисте життя», який відповідає міжнародному стандарту *ISO*/*IEC* 29100:2011. Для ІС, які знаходяться у приватній власності і обробляють персональні дані, власники додатково можуть прийняти рішення щодо впровадження відповідності ІС вимогам міжнародних Регламентів (*GDPR*).

<table>
<tr><td colspan="2" rowspan="3">Типи інформації
Типи ІС</td><td colspan="4">Інформація з обмеженим доступом</td><td rowspan="3">Відкрита інформація</td></tr>
<tr><td colspan="2">Секретна</td><td colspan="2">Критична інформація</td><td rowspan="2">Персональні дані</td></tr>
<tr><td colspan="2">Гриф секретності</td><td colspan="2">Рівень критичності</td></tr>
<tr><td colspan="2"></td><td>Т | ЦТ | ОВ</td><td>Високий | Середній | Низький</td><td></td><td></td></tr>
<tr><td colspan="2">Державні ІС</td><td>Комплексні системи захисту інформації (КСЗІ)</td><td colspan="2">СБІ відповідно до національних вимог + державна авторизація</td><td>СБІ відповідно до національних вимог Додаткові вимоги ДСТУ 7731:2015</td><td>СБІ</td></tr>
<tr><td rowspan="2">ОКІ</td><td>І/ІІ категорія критичності</td><td rowspan="2">КСЗІ</td><td colspan="2">СБІ відповідно до національних вимог + державна авторизація</td><td rowspan="2">СБІ відповідно до національних вимог Додаткові вимоги ДСТУ 7731:2015</td><td rowspan="2">СБІ</td></tr>
<tr><td>ІІІ/IV категорія критичності</td><td colspan="2">СБІ відповідно до національних /міжнародних вимог + державна авторизація</td></tr>
<tr><td colspan="2">ІС у приватній власності</td><td>КСЗІ</td><td colspan="2">СБІ відповідно до національних/міжнародних вимог</td><td>СБІ відповідно до національних вимог Додаткові вимоги ДСТУ 7731:2015 / GDPR</td><td>СБІ</td></tr>
<tr><td colspan="2" rowspan="2">Класифікація ІС</td><td rowspan="2">Відповідно до НД ТЗІ 2.5-005 - 99
АС клас 1
АС клас 2
АС клас 3</td><td colspan="3">Відповідно до НД ТЗІ 3.6-004-21</td><td rowspan="2">-</td><td rowspan="2">-</td></tr>
<tr><td>ІС з високою категорією критичності</td><td>ІС з середньою категорією критичності</td><td>ІС з низькою категорією критичності</td></tr>
</table>

Рисунок 2.1 – Модель впровадження системи безпеки інформації [67]

Державні ІС, у яких циркулює критична інформація, мають розгортати СБІ керуючись положеннями НД ТЗІ 3.6-004 [67] для впровадження відповідних заходів захисту, направлених на забезпечення конфіденційності, цілісності та доступності критичної інформації, яка циркулює у таких ІС.

ІС на ОКІІ І-ІІ категорії критичності мають розгортати СБІ керуючись положеннями НД ТЗІ 3.6 -004 [67], а на ОКІІ ІІІ - IV категорії критичності можуть розгортати СБІ або керуючись НД ТЗІ 3.6 -004, або положеннями міжнародних стандартів. ІС, у яких циркулює секретна інформація, мають розгортати КСЗІ, керуючись вимогами чинної національної нормативно-правової бази.

Незалежно від категорії критичності ОКІ, ІС, у яких циркулює критична інформація, мають проходити процедуру державної авторизації розгорнутих на них СБІ.

2.2 Категоризація

2.2.1 Категоризація об’єктів критичної інфраструктури

Як випливає з рис.2.1 категорія ОКІІ впливає на склад нормативно-правової бази розробки системи захисту і, відповідно, на склад і зміст документації, яка оформлюється в процесі розробки.

Категорія критичності визначається для ОКІ, ОКІІ та ІС у послідовності рис.2.2.

Рисунок 2.2 – Визначення категорій критичності

Властивості морської галузі як складової критичної інфраструктури України були визначені шляхом аналізу Постанови Кабінету міністрів України №1109 2020 року в редакції 24-го року [24].

Морська галузь включає в себе морський та внутрішній водний транспорт із портами включно. Крім того, функціонування водного транспорту неможливе без якісного ремонту суден і організації заміни транспортного парку, тобто без суднобудування. Тому ці дві галузі з точки зору стійкості функціонування воднотранспортного комплексу доцільно розглядати разом.

Морський і внутрішній водний транспорт та суднобудування за Постановою Кабінету міністрів України №1109 (в редакції 24-го року [24]) є підсекторами різних секторів КІ України і, відповідно, мають різні секторальні органи у сфері захисту КІ та надають різні основні послуги (табл.2.1). «Морський і внутрішній водний транспорт» відноситься до сектору КІ України «Транспорт і пошта», а «Суднобудування» - до сектору «Промисловість»

Таблиця 2.1 – Порівняння підсекторів КІ «Морський та внутрішній водний транспорт» та «Суднобудування»

Характеристики	Морський та внутрішній водний транспорт	Суднобудування
Сектор	Транспорт і пошта	Промисловість
Секторальний орган у сфері захисту КІ	Міністерство інфраструктури (Мінінфраструктури)	Міністерство з питань стратегічних галузей промисловості України (Мінстратегпром)
Основні послуги	–здійснення контролю та нагляду за безпекою судноплавства та мореплавства; –інжинірингова діяльність для будівництва, ефективного використання та утримання об'єктів портової інфраструктури, розташованих у межах території та акваторії морського порту; –обслуговування суден, що заходять до морських, річкових портів (терміналів) України, пасажирів, вантажів (вантажно-розвантажувальні роботи, обслуговування, зберігання, перевезення вантажів, пасажирів); –обслуговування та утримання внутрішніх водних шляхів, об'єктів інфраструктури внутрішнього водного транспорту; –виконання міжнародних зобов'язань України у тому числі:	суднобудування та постачання продукції суднобудування

Продовження таблиці 2.1

Характеристики	Морський та внутрішній водний транспорт	Суднобудування
	–лоцманське проведення суден –регулювання руху суден; –технічний нагляд за суднами; –пошук і рятування людей в морі; гідрографічне забезпечення.	
Кількість міжсекторальних критеріїв оцінювання рівнів критичності ОКІ	15	15
Максимальна сумарна оцінка рівнів критичності ΣPK_{max}	68	68

Критичність ОКІ оцінюється за різними секторальними критеріями (табл.2.2 і табл..2.3), однак загальна кількість секторальних і міжсекторальних критеріїв і, відповідно, максимальна сумарна оцінка критичності для них однакові (табл..2.1).

Таблиця 2.2 – Секторальний критерій оцінювання критичності ОКІ в підсекторі «Морський та внутрішній водний транспорт»

Фактор негативного впливу в підсекторі	Критерій оцінювання негативного впливу		
	Умова	Рівень негативного впливу	Оцінка PK_i
Знищення, пошкодження або порушення функціонування ОКІ	не застосовується	незначні наслідки	1 бал
	час припинення надання морських послуг у морських портах може становити не більше як 24 години	значні наслідки	2 бала
	час припинення надання морських послуг у морських портах може становити від 24 до 72 годин	критичні наслідки	3 бали
	припинення надання морських послуг у морських портах більш як на 72 години (Правила надання послуг у морських портах України, затверджені наказом Мінінфраструктури від 5 .06.2013 р. № 348)	катастрофічні наслідки	4 бала

Таблиця 2.3 – Секторальний критерій оцінювання критичності ОКІ в підсекторі «Суднобудування»

Фактор негативного впливу в секторі	Критерій оцінювання негативного впливу		
	Умова	Рівень негативного впливу	Оцінка $РК_i$
Знищення, пошкодження або порушення функціонування ОКІ призведе до ненадання об'єктом основних послуг	для менш як 6000 жителів	незначні наслідки	1 бал
	для більш як 6000 жителів	значні наслідки	2 бала
	для більш як 30 000 жителів на території області або більш як одного району міста - обласного центру, або на всій території одного міста обласного значення	критичні наслідки	3 бали
	для більш як 100 000 жителів на території більш як однієї області або не менш як трьох міст обласного значення	катастрофічні наслідки	4 бала

Міжсекторальні критерії оцінювання критичності ОКІ, які для обох підсекторів є однаковими [24, 56], призначені для оцінки тяжкості потенційних наслідків порушень штатного функціонування ОКІ для окремих осіб, економіки, екології та соціуму. Вони визначаються за різними показниками – за потенційною кількістю смертельних випадків, значимістю потенційних економічних втрат і негативного впливу на суспільну довіру, впливом на інші сектори КІ тощо.

Категорія критичності присвоюється ОКІ відповідно до Закону України «Про критичну інфраструктуру» [96] спеціальною робочою групою, створеною в межах підсектора «Морський та внутрішній водний транспорт», і є якісною експертною оцінкою діапазону, до якого належить ступінь важливості, який визначається кількісним оцінюванням тяжкості наслідків порушення штатного функціонування об'єкта оцінювання і виконання ним його основних функцій за секторальними і міжсекторальними критеріями.

Категоризацію проводить робоча група, яка утворюється в межах сектору або підсектору КІ за наказом уповноваженого органу, і до складу якої є певні нормативні вимоги.

Згідно із затвердженою методикою категоризації ОКІ [24, 56] робочою групою в межах її відповідальності для кожного об'єкта КІ визначаються експертні оцінки його критичності $РК_i$ за всіма критеріями (для підсекторів

«Суднобудування» та «Морський та внутрішній водний транспорт» $i = \overline{1,16}$) і розраховується узагальнена нормована оцінка критичності $РК_{ОКІ}$ за формулою:

$$PK_{OKI} = \frac{\sum\limits_{i=1}^{16} PK_i}{\sum\limits_{i=1}^{16} PK_{i\_\max}} = \frac{\sum\limits_{i=1}^{16} PK_i}{68}. \qquad (2.1)$$

Об’єктам інфраструктури може бути присвоєна одна із чотирьох категорій критичності за діапазоном значень, в який потрапляє $РК_{ОКІ}$:

якщо $0,8 < РК_{ОКІ} \leq 1$, то - I категорія критичності (об’єкт є особливо важливим;

якщо $0,63 < РК_{ОКІ} \leq 0,8$, то - II категорія критичності (об’єкт є життєво важливим);

якщо $0,37 < РК_{ОКІ} \leq 0,63$, то - III категорія критичності (об’єкт є важливим);

якщо $0,2 < РК_{ОКІ} \leq 0,37$, то - IV категорія критичності (об’єкт є необхідним);

якщо $РК_{ОКІ} \leq 0,2$, то об'єкт не є критичним.

Критичність об’єктів інформаційної інфраструктури, які входять до складу ОКІ, визначається за окремими правилами:

а) якщо кібератака на об’єкт інформаційної інфраструктури (на комунікаційну або технологічну систему) ОКІ впливає на стале функціонування ОКІ і виконання ним основних функцій, то цей об’єкт інформаційної інфраструктури (за Законом України «Про основні засади забезпечення кібербезпеки України» [97]) є ОКІІ ОКІ;

б) ОКІІ присвоюється та ж сама категорія критичності, що й ОКІ в разі виконання всіх наступних умов (визначені в «Порядку формування переліку об’єктів критичної інформаційної інфраструктури» [23]) якщо:

– об’єкт є необхідними для стійкого та безперервного функціонування ОКІ та для надання ОКІ основних послуг;

– інцидент з інформаційної безпеки на об’єкті істотно впливає на безперервність та стійкість надання ОКІ основних послуг;

– відсутній альтернативний об’єкт (спосіб) для надання ОКІ тих послуг, що надає даний об’єкт.

2.2.2 Категоризація інформаційних систем за НД ТЗІ 3.6-004-21

Згідно НД ТЗІ 3.6-004-21 [67] процес впровадження системи безпеки інформації містить етап категоріювання безпеки, на якому всім активам ІС на основі її опису мають бути присвоєні рівні критичності (низький, середній та високий). Критичність оцінюється за рівнем негативного впливу наслідків порушення конфіденційності, цілісності та доступності активів ІС. Рівень критичності визначається за оцінками за визначеними критеріями негативного впливу за кожною властивістю безпеки. Порядок оцінювання критичності та порядок проведення категоріювання встановлюються НД ТЗІ 3.6-005-21 «Порядок категоріювання безпеки інформаційної системи та інформації» [68].

В НД ТЗІ 3.6-005-21 [68] категоріювання безпеки ІС розглядається як один з етапів менеджменту ризиків інформаційної безпеки при створенні СБІ за моделлю ПВПД (плануй – виконуй – перевіряй – дій). В процесі категоріювання виконуються три завдання, кожне з яких має низку підзадач:

К-1. Опис інформаційної системи:

К-1.1. Документування організаційної належності ІС;

К-1.2. Документування процедур, функцій, активів, прикладних процесів ІКС;

К-1.3. Визначення дійових осіб ІС: ролі дійових осіб (Користувач, Системний адміністратор, Адміністратор безпеки, Власник (розпорядник) ІКС), статуси дійових осіб за ролями (Внутрішній, Зовнішній), авторизовані привілеї та функції, що виконуються (право на користування ресурсами ІС, право на перегляд і додавання нових користувачів, право на визначення політики обліку й управління персоналом, що використовує ІС);

К-1.4. Розроблення варіантів використання ІС;

К-1.5. Інвентаризація ІТ-активів. До складу ІТ-активів відносяться: інформаційні системи, активні мережеві компоненти, окремі робочі станції, обладнання, програмного забезпечення тощо.

Активи, що є апаратним забезпеченням, описуються наступними відомостями:

– «унікальна назва ІТ-активу;

– опис ІТ-активу (тип і функція (призначення), наприклад: поштовий сервер, веб-сервер, маршрутизатор, робоча станція тощо);

– платформа (наприклад, апаратна архітектура/операційна система);

– кількість ІТ-активів (систем), згрупованих разом;

– місце установки ІТ-активу;

– статус ІТ-активу (операційна, тестова фаза, планування);

– дійові особи, які допущені до ІТ-активу» [68].

Активи, що є програмним забезпеченням, описуються наступними відомостями:

– код;

– найменування;

– опис;

– місце установки на визначених компонентах ІС;

– функції (процеси), у яких даний актив застосовується;

К-1.6. Інвентаризація типів інформації, що обробляється в інформаційній системі. Типи інформації описуються наступними відомостями:

– ідентифікатор типу інформації;

– назва типу інформації;

– повний опис інформації;

– застосовувані процеси та функції;

К-2. Категоріювання безпеки:

Крок 1. Визначення рівня критичності (РК) кожного типу інформації, що обробляється в ІС, за ступенем потенційної шкоди власнику інформації чи

організації внаслідок порушення вимог безпеки (конфіденційності, цілісності та доступності інформації). Рівень негативного впливу визначається власником/розпорядником інформації (самостійно, із залученням експертів або іншими методами) окремо за кожною вимогою безпеки. РК визначається як якісний показник: $РК \in$ {Низький, Середній, Високий}. $РК$=Низький відповідає обмеженому негативному впливу, $РК$=Середній – відчутному (серйозному впливу, а $РК$=Високий – критичному чи навіть катастрофічному впливу. В результаті отримують множину $\{РК_{\text{тип, конфіденційність}}, РК_{\text{тип, цілісність}}, РК_{\text{тип, доступність}}\}$. РК для інформації певного типу визначається за правилом:

$$РК_{\text{тип}}=\max\{РК_{\text{тип, конфіденційність}}, РК_{\text{тип, цілісність}}, РК_{\text{тип, доступність}}\}. \quad (2.2)$$

В якості типів інформації в розглядаються інформаційні активи. Тому при наявності множини з n активів $A=\{IA_i\}$, $i=\overline{1,n}$ отримуємо множину оцінок їх рівнів критичності $РКА=\{РК_i\}$.

Крок 2. Визначення категорії критичності ($КК$) ІКС за правилом $КК_{ІКС}=\max\{РК_i\}$, тобто $КК_{ІКС}$ визначається як максимальний $РК$ серед усіх інформаційних активів ІКС.

К-3. Аналіз і ухвалення рішення за результатами категоріювання безпеки ІС та інформації:

Крок 1. Документування результатів категоріювання безпеки. Форму та за зміст документації, що складається за результатами категоріювання безпеки, визначають внутрішні розпорядчі документи організації-власника/розпорядника ІКС, однак обов’язково мають бути задокументовані наступні відомості:

– найменування ІКС, її приналежність до КІ і ОКІ та надання життєво важливої послуги;

– типи інформації, що обробляються ІКС, та їх характеристика з точки зору необхідності для надання життєво важливої послуги, бізнес-процесів, виконання завдань організації за призначенням тощо;

– обґрунтування за кожним типом інформації рівня негативного впливу на виконання функцій організацією за у випадку порушення вимог безпеки (конфіденційності, цілісності, доступності інформації певного типу);

– визначення рівня критичності ІКС;

– в якості додатків - інша інформація (опис ІКС, функцій і завдань організації за призначенням, взаємодії організації з іншими об’єктами (наприклад ОКІ тощо), яка необхідна керівництву для оцінювання валідності наданих результатів;

Крок 2. Аналіз результатів категоріювання безпеки – перевірка керівництвом (власником/розпорядником інформаційної системи) валідності наданих результатів;

Крок 3. Ухвалення рішення за результатами категоріювання безпеки: затвердження результатів категоріювання безпеки (присвоєння ІКС певної категорії критичності) та використання їх для вибору базового профілю безпеки та розробки цільового профілю безпеки.

2.2.3 Визначення ступеня критичності комп’ютеризованих систем в морській галузі за *IACS UR E*22

Категорія критичності комп’ютеризованої системи в морській галузі визначається згідно із *IACS UR E*22 [3] в залежності тяжкості наслідків виходу системи з ладу: перша категорія присвоюється, якщо вихід з ладу системи не призведе до небезпечних ситуацій для безпеки людини, судна та/або до загрози для навколишнього середовища, друга – якщо може призвести, а третя – якщо обов’язково призведе (табл..2.4).

Таблиця 2.4 – Категорії критичності комп’ютерних систем за *IACS UR E*22 «*Computer-based systems*»

Категорія	Негативні наслідки:	Типова функціональність систем
I	Системи, вихід з ладу яких не призведе до небезпечних ситуацій для безпеки людини, судна та/або до загрози для навколишнього середовища	Моніторинг, інформаційна та адміністративна функції

Продовження таблиці 2.4

Категорія	Негативні наслідки:	Типова функціональність систем
II	Системи, вихід з ладу може призвести до небезпечних ситуацій для безпеки людини, судна та/або до загрози для навколишнього середовища	Суднова тривога, функції моніторингу і управління, які необхідні для підтримки судна в нормальному стані для експлуатації та проживання
III	Системи, збій у роботі яких негайно призведе до небезпечних або катастрофічних ситуацій для безпеки людини, судна та/або до загрози для навколишнього середовища	Управління рухом судна, рульове керування, функції безпеки судна

Системи категорії I не є небезпечними і не перевіряються Класифікаційним товариством, але щодо них може надходити запит на інформацію, яка необхідна, щоб підтвердити їх категорію або гарантувати, що вони не впливають на роботу систем категорії II та категорії III.

Категорії оцінюються в контексті, тому категорії однієї комп'ютерної системи на різних суднах можуть бути різними.

Результати всіх процесів категоризації оформлюються у вигляді акту категоризації.

2.3 Документаційний супровід етапів створення КСЗІ

Порядок проведення робіт зі створення КСЗІ в ІКС передбачає проведення низки етапів робіт, кожен з яких супроводжується власним комплектом документів. Роботи починаються з формування вимог до КСЗІ і завершуються державною експертизою КСЗІ.

Вимоги до складу і змісту документів на кожному етапі створення КСЗІ наведені в табл.2.5.

Таблиця 2.5 - Вимоги до складу і змісту документів на етапах створення комплексної системи захисту інформації

Кроки			Документи	
№	Назва	Зміст робіт	Документ	Зміст документа
Етап 1. Формування загальних вимог до КСЗІ в ІКС				
1.1	Обґрунтування необхідності створення КСЗІ	Аналіз нормативно-правових актів Виявлення ІзОД та інформації, для якої має забезпечуватися цілісність і доступність Оцінка можливих переваг (фінансово-економічних, соціальних тощо) експлуатації ІКС у разі створення КСЗІ.	Рішення про створення КСЗІ	Обґрунтування необхідності (за властивостями інформації і нормативно-правовою базою) і доцільності (з економічної, соціальної або іншої точки зору) створення КСЗІ
1.2	Обстеження середовищ функціонування ІКС	Опис кожного середовища функціонування ІКС та виявлення в ньому елементів, які безпосередньо чи опосередковано можуть впливати на безпеку інформації Виявлення взаємного впливу елементів різних середовищ. Описуються: середовище функціонування ІКС, інформаційне середовище, фізичне середовище, середовище користувачів	Концепція ІКС	Основні принципи і підходи до побудови ІКС
			Концепція безпеки інформації	Визначені наміри керівництва щодо функцій і ролі ІКС в організації та щодо обробки і прийняття ризиків
			Перелік об’єктів захисту	Список об’єктів захисту із визначеними характеристиками (розташування, властивості інформації, користувачі, зв'язок з іншими об’єктами і з процесами)
			Модель загроз	Відповідно до положень НД ТЗІ 1.1-002-99 та НД ТЗІ 1.4-001-2000 [62]. Модель загроз для інформації та модель порушника рекомендується оформляти у вигляді окремих документів (або поєднаних в один документ) Плану захисту.
			Модель порушника	
			План захисту	Згідно з НД ТЗІ 1.4-001-2000 [62]
			Акт обстеження	Фіксація факту проведення обстеження

Продовження таблиці 2.5

Кроки			Документи	
№	Назва	Зміст робіт	Документ	Зміст документа
1.3	Формування завдання на створення КСЗІ	Визначення завдань ЗІ в ІКС, мети створення КСЗІ, варіантів вирішення завдань захисту (відповідно до ДСТУ 3396.1-96), основних напрямів забезпечення захисту Аналіз ризиків Визначення переліку суттєвих загроз. Визначення загальної структури та складу КСЗІ, вимог до можливих заходів, методів та засобів ЗІ, обмежень щодо застосування певних заходів і засобів захисту та щодо використання ресурсів ІКС для реалізації завдань захисту, припустимих витрат на створення КСЗІ, умов створення, введення в дію і функціонування КСЗІ (окремих її підсистем, компонентів), загальних вимог до співвідношення та меж застосування в ІКС (окремих її підсистемах, компонентах) організаційних, інженерно-технічних, технічних, криптографічних та інших заходів захисту інформації, що ввійдуть до складу КСЗІ.	Перелік суттєвих загроз	Перелік загроз із визначеними ризиками. Виділення прийнятних ризиків і ризиків, що вимагають обробки
			Звіт про виконання робіт із формування завдання на створення КСЗІ	Результати виконаних робіт і висновки: суттєві загрози, загальна структура і склад КСЗІ, обмеження на вибір організаційних і технічних рішень, вимоги до компонентів КСЗІ
			Заявка на розробку КСЗІ	Тактико-технічне завдання на створення КСЗІ
Етап 2. Розробка політики безпеки інформації в ІКС				
2.1	Вивчення об’єкта, на якому створюється КСЗІ, проведення науково-дослідних робіт	Розробник КСЗІ проводить Детальне вивчення Розробником об’єкта, на якому створюється КСЗІ, уточнення моделі загроз, моделі потенційного порушника та результатів аналізу можливості керування ризиками, виконання у разі потреби додаткові науково-дослідні роботи, пов’язаних з пошуком шляхів реалізації завдання на створення КСЗІ, оформлення і затвердження звітів з науково-дослідних робіт, що виконувалися.	Перелік суттєвих загроз	Уточнений перелік загроз із визначеними ризиками. Виділення прийнятних ризиків і ризиків, що вимагають обробки
			Модель загроз	Уточнена модель загроз
			Модель порушника	Уточнена модель порушника
			Звіти з науково-дослідних робіт	Згідно з тематикою робіт
2.2	Вибір варіанта КСЗІ	Підготовка альтернативних варіантів концепції створення КСЗІ і планів їх реалізації, оцінка переваг і недоліків кожного варіанта, вибір оптимального варіанта.	Звіт	Концепція оптимального варіанта КСЗІ

Продовження таблиці 2.5

Кроки			Документи	
№	Назва	Зміст робіт	Документ	Зміст документа
2.3	Оформлення політики безпеки	Вибір основних рішень з протидії всім суттєвим загрозам. Формування загальних вимог, правил, обмежень, рекомендацій тощо, які регламентують використання захищених технологій обробки інформації в ІКС, окремих заходів і засобів захисту інформації, діяльність користувачів усіх категорій Документальне оформлення політики безпеки інформації. Політика безпеки може розроблятися для ІКС в цілому або, якщо мають місце особливості функціонування окремих компонентів КСЗІ, для окремої компоненти, для окремого функціонального завдання, для окремої технології обробки інформації тощо.	Політика (політики) безпеки	Згідно з положеннями НД ТЗІ 1.1-002-99 та рекомендаціями НД ТЗІ 1.4-001-2000 [62]. Політику безпеки рекомендується оформляти у вигляді окремого документа Плану захисту
Етап 3. Розробка технічного завдання на створення КСЗІ				
3.1	Розробка і оформлення технічного завдання	Об’єднання в єдину систему усіх необхідних заходів і засобів захисту від різноманітних загроз безпеці інформації на всіх етапах життєвого циклу ІКС. Вибір варіанта виконання технічного завдання: - окремий розділ технічного завдання на створення ІКС (для нових ІУС); - окреме (часткове) технічне завдання (при модернізації КСЗІ); - доповнення до технічного завдання на створення ІКС (для ІКС, технічне завдання на які не містить розділу щодо ЗІ). Для інтегрованих ІКС, які будуються за модульним принципом, вимоги до КСЗІ кожної зі складових частин ІКС рекомендується оформляти окремим документом.	Технічне завдання на створення КСЗІ	Зміст, порядок погодження та затвердження технічного завдання повинні відповідати НД ТЗІ 3.7-001-99

Продовження таблиці 2.5

Кроки			Документи	
№	Назва	Зміст робіт	Документ	Зміст документа
		Дозволяється готувати один документ на декілька однотипних складових частин КСЗІ, вказавши існуючі між ними відмінності чи особливості		
Етап 4. Розробка проєкту КСЗІ				
4.1	Ескізний проєкт	Визначаються: функції КСЗІ в цілому та функції її окремих складових частин; склад комплексів технічного захисту інформації від витоку технічними каналами та від спеціальних впливів; склад заходів протидії технічним розвідкам, організаційних, правових та інших заходів захисту; склад КЗЗ; узагальнена структура КСЗІ та схема взаємодії складових частин. Пропонуються попередні технічні рішення, за допомогою яких передбачається реалізація завдань і функцій КСЗІ.	Ескізний проект	Попередні технічні рішення для реалізації завдань і функцій КСЗІ. Склад документації визначається технічним завданням на КСЗІ та НД ТЗІ 2.5-004-99 [64]
4.2	Технічний проєкт	Розробка: загальних проєктних рішень, необхідних для реалізації вимог технічного завдання на КСЗІ; рішень щодо структури КСЗІ (організаційної структури, структури технічних і програмних засобів), алгоритмів функціонування та умов використання засобів захисту; рішень щодо архітектури КЗЗ та механізмів реалізації, визначених функціональним профілем послуг безпеки інформації. Проведення організаційно-технічних заходів щодо забезпечення послідовності розробки КЗЗ, архітектури, середовища розробки, випробувань, середовища функціонування та експлуатаційної документації КЗЗ відповідно до заданих рівнем гарантій реалізації послуг безпеки згідно зі специфікаціями НД ТЗІ 2.5-004-99 [64].	Технічний проєкт	Загальні проєктні рішення, які необхідні для реалізації вимог технічного завдання на КСЗІ. Склад документації - згідно із технічним завданням на КСЗІ та НД ТЗІ 2.5-004-99 [64]
			Документація на КСЗІ	В обсязі, передбаченому технічним завданням на КСЗІ і достатньому для опису проектних рішень
			Документації на постачання для комплектації КСЗІ	Документація на постачання засобів захисту або продукції, що містить їх у своєму складі

Продовження таблиці 2.5

Кроки			Документи	
№	Назва	Зміст робіт	Документ	Зміст документа
		Розробка документації на КСЗІ: - розробка, оформлення, узгодження та затвердження документації в обсязі, передбаченому технічним завданням на КСЗІ і достатньому для опису проектних рішень; - підготовка та оформлення документації на постачання засобів захисту або продукції, що містить їх у своєму складі, для комплектації КСЗІ. Якщо необхідної продукції немає на ринку засобів захисту, то визначаються технічні вимоги (складаються технічні завдання) на розроблення відповідних засобів; - розробка, оформлення і затвердження завдань на проєктування і суміжних питань, які пов'язані зі створенням КСЗІ або впливають на умови її функціонування	Технічні завдання на розробку засобів захисту	Технічні вимоги у вигляді технічних завдань на розробку засобів захисту, відсутніх на ринку
			Завдання на проектування і вирішення суміжних питань	Завдання на будівельні роботи
				Завдання на електротехнічні роботи
				Завдання на санітарно – технічні роботи
				Завдання на інші підготовчі роботи
4.3	Робочий проєкт	Розробка, оформлення та затвердження робочої та експлуатаційної документації КСЗІ та у разі потреби її окремих складових частин. Розробка засобів захисту інформації, відсутніх на ринку або адаптація готової продукції до умов функціонування КСЗІ. Розробка засобів захисту інформації від НСД проводиться згідно з НД ТЗІ 3.6-001-2000. .	Робочий проєкт	Детальні рішення щодо реалізації технічного проєкту КСЗІ. Склад документації - згідно із технічним завданням на КСЗІ та НД ТЗІ 2.5-004-99 [64]
			Робоча документація	Детальні рішення щодо реалізації технічного проєкту КСЗІ, забезпечення управління КСЗІ і взаємодії її компонентів; документація, яка необхідна для тестування, проведення пусконалагоджувальних робіт і проведення випробувань КСЗІ. Описи процедур інсталяції та ініціалізації комплексу,

Продовження таблиці 2.5

Кроки			Документи	
№	Назва	Зміст робіт	Документ	Зміст документа
				налагодження механізмів розмежування доступу користувачів до інформації та апаратних ресурсів ІКС, контролю за діями користувачів, формування та актуалізації баз даних захисту, а також контролю цілісності програмного забезпечення та баз даних захисту. Вихідні дані для внесення їх до баз даних захисту.
			Експлуатаційна документація	Опис порядку функціонування КСЗІ та настанови (інструкції) щодо забезпечення цього порядку обслуговуючим персоналом і користувачами, порядку супроводження КСЗІ впродовж життєвого циклу ІКС
Етап 5. Введення КСЗІ в дію та оцінка захищеності інформації в ІКС				
5.1	Підготовка КСЗІ до введення в дію	Розробка розпорядчих документів, що регламентують діяльність із забезпечення захисту інформації в ІКС. Створення служби захисту інформації. Завершення розробки і затвердження документів, що входять до Плану захисту (за виключенням тих, для розробки яких необхідні результати наступних етапів робіт). Створення Плану захисту	Розпорядчі документи	Порядок діяльності із забезпечення ЗІ в ІКС
			Накази про створення служби захисту інформації	Згідно НД ТЗІ 1.4-001-2000 [62]: склад служби, посадові обов'язки і права, правила взаємодії з підрозділами організації і з іншими організаціями
			План захисту	Згідно з НД ТЗІ 1.4-001-2000 [62]
5.2	Навчання користувачів	Навчання користувачів ІКС всіх категорій (технічного обслуговуючого персоналу, звичайних користувачів та користувачів, які мають повноваження щодо управління	Документи, отримані користувачами,	Терміни навчання, місце навчання, зміст навчальних курсів, оцінка результатів

Продовження таблиці 2.5

Кроки			Документи	
№	Назва	Зміст робіт	Документ	Зміст документа
		засобами КСЗІ, тощо) в частині, що їх стосується, основним положенням документів Плану захисту, які необхідні їм для дотримання правил політики безпеки інформації, експлуатації засобів захисту інформації тощо. Перевірка і реєстрація результатів навчання.	де фіксуються результати навчання	навчання і /або висновок щодо допуску до роботи
5.3	Комплектування КСЗІ	Отримання комплектуючих КСЗІ від постачальників та співвиконавців робіт (засобів захисту інформації, матеріалів, обладнання та іншого). Прийняття рішення щодо підготовки до проведення оцінки на відповідність вимогам НД ТЗІ засобів захисту, які на момент проєктування КСЗІ не мали відповідного сертифіката або експертного висновку. Прийняття рішення щодо порядку проведення такої оцінки під час державної експертизи КСЗІ.	Акти прийомки-передавання	Комплектуючі, дата отримання, вартість, постачальник, отримувач поставки, постановка на облік, розміщення на складі
			Рішення про оцінку відповідності засобів захисту	Перелік засобів захисту без сертифікатів або експертних висновків. Порядку проведення їх оцінки під час державної експертизи КСЗІ
5.4	Будівельно-монтажні роботи	Розробка проєктною організацією проєктної документації на будівництво відповідно до вимог ДБН 2.2-3-2012 Проведення будівельних робіт силами організації-власника ІКС або будівельно-монтажних організацій згідно з проєктною документацією на будівництво. Створення комісії з прийняття будівельних робіт після їх завершення, до складу якої входять представники організації-замовника будівельних робіт, проєктної та будівельно-монтажної організацій. Перевірка якості виконаних робіт і складання акта приймання робіт	Акт приймання робіт	Фіксація завершення робіт, оцінка їх відповідності вимогам ТЗІ. Акт затверджується керівником організації-замовника будівництва
5.5	Пусконалагоджувальні роботи	Монтаж обладнання. Визначення мінімально допустимих відстаней між основними технічними засобами, які не мають сертифіката	Протоколи спеціальних досліджень та	Умови проведення, застосовані технічні і програмні засоби, результати спеціальних досліджень

Продовження таблиці 2.5

Кроки			Документи	
№	Назва	Зміст робіт	Документ	Зміст документа
		або експертного висновку про відповідність вимогам з ТЗІ, та допоміжними технічними засобами за результатами їх спеціальних досліджень.	інструментальних вимірювань рівня ПЕМВН	та інструментальних вимірювань рівня ПЕМВН
		Спеціальні дослідження та інструментальні вимірювання рівня ПЕМВН підрозділом ТЗІ організації-власника ІКС або іншими суб'єктами господарювання за умови наявності ліцензії чи дозволу на проведення відповідного виду робіт Оцінка відповідності проведення монтажних робіт вимогам експлуатаційних документів на засоби та НД ТЗІ 3.6-003-2016. Розробка пропозицій щодо застосування додаткових заходів захисту, впровадження яких є необхідним у разі неможливості під час виконання монтажних робіт дотримання окремих вимог із розміщення основних технічних засобів. Складання акту відповідності монтажних робіт Впровадження додаткових засобів захисту, визначених в акті відповідності монтажних робіт, і відповідне коригування проектної, робочої та експлуатаційної документації. Атестація комплексу технічного захисту інформації від витоку технічними каналами. Інсталяція, ініціалізація та перевірка працездатності КЗЗ згідно з документацією робочого проєкту. Внесення записів до бази даних захисту Перевірка працездатності засобів захисту інформації в автономному режимі та при їх комплексній взаємодії.	Акт відповідності монтажних робіт	Категорії приміщень, де розташоване обладнання ІКС, межі контрольованих зон для приміщень, перелік основних і додаткових технічних засобів та комунікацій (із зазначенням найменування, типу, заводського номера) у цих приміщеннях. Оцінка відповідності монтажних робіт вимогам експлуатаційних документів на засоби та НД ТЗІ 3.6-003-2016. Пропозиції щодо застосування додаткових заходів захисту, впровадження яких є необхідним у разі неможливості під час виконання монтажних робіт дотримання окремих вимог із розміщення ОТЗ. Акт затверджується керівником організації - власника ІКС
			Коригована проєктна, робоча, експлуатаційна документація КСЗІ	Проєктна, робоча, експлуатаційна документація КСЗІ, відкоригована за результатами впровадження додаткових засобів захисту

Продовження таблиці 2.5

Кроки			Документи	
№	Назва	Зміст робіт	Документ	Зміст документа
			Акт атестації КТЗІ від витоку технічними каналами	Оцінка повноти та якості виконання робіт з технічного захисту інформації від витоку технічними каналами
			Записи в базі даних захисту	Відомості про користувачів ІКС, їх повноваження щодо доступу до захищених об'єктів ІКС, їх створення, модифікації, архівування, знищення, експорту/імпорту із системи та інші дані
5.6	Попередні випробування	Перевірка працездатності КСЗІ, її відповідності технічному завданню і можливості прийняття КСЗІ у дослідну експлуатацію. Програму й методики випробувань готує розробник КСЗІ, а узгоджує замовник ІКС. Попередні випробування організовує замовник ІКС, а проводить розробник КСЗІ спільно із замовником. Для цього замовником ІКС створюється комісія, головою якої призначається представник замовника. Результати попередніх випробувань, які можуть виявити недоліки КСЗІ оформлюються протоколом випробувань. Після усунення недоліків у випадку їх наявності та оформлюється акт про приймання КСЗІ у дослідну експлуатацію.	Програма випробувань Методики випробувань	Згідно з вимогами РД 50-34.698-90 [99]
			Протокол випробувань	Висновок щодо можливості прийняття КСЗІ у дослідну експлуатацію. Перелік виявлених недоліків, необхідних заходів з їх усунення, і рекомендовані терміни виконання цих робіт
			Коригована проєктна, робоча, експлуатаційна документація КСЗІ	Проєктна, робоча, експлуатаційна документація КСЗІ, відкоригована за результатами попередніх випробувань
			Акт про приймання КСЗІ у дослідну експлуатацію	Висновок про приймання КСЗІ у дослідну експлуатацію

Продовження таблиці 2.5

Кроки			Документи	
№	Назва	Зміст робіт	Документ	Зміст документа
5.7	Дослідна експлуатація	Відпрацьовування технології оброблення інформації, обігу машинних носіїв інформації, керування засобами захисту, розмежування доступу користувачів до ресурсів ІКС та автоматизованого контролю за діями користувачів. Набуття співробітниками СЗІ та користувачами ІКС практичних навичок з використання технічних та програмно-апаратних засобів ЗІ, засвоєння ними вимог організаційних та розпорядчих документів з питань розмежування доступу до технічних засобів та інформаційних ресурсів. У разі потреби - доопрацювання програмного забезпечення, додаткове налагоджування та конфігурування КЗЗ; коригування робочої та експлуатаційної документації.	Акт про завершення дослідної експлуатації	Висновок щодо можливості /неможливості подання КСЗІ на державну експертизу.
5.8	Державна експертиза КСЗІ	Проведення державної експертизи. Виявлення недоліків. Усування недоліків. Якщо через якісь причини усунути недоліки в ході експертизи неможливо, це оформлюється актом, до якого вноситься перелік необхідних доробок та рекомендації щодо їх виконання. Після завершення передбачених актом робіт проводиться повторна експертиза.	Атестат відповідності	Висновок про відповідність КСЗІ нормативно визначеним вимогам
			Акт	Перелік необхідних доробок та рекомендації щодо їх виконання. Висновок щодо проведення повторної експртизи
	Оцінювання СБІ	Оцінювання СБІ незалежним оцінювачем за НД ТЗІ 2.3-025-21 «Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем» [63]	Звіт оцінювача	Висновок про правильність визначення цільового профілю Висновок про правильність вибору заходів захисту Висновок про відповідність СБІ цільовому профілю.

Продовження таблиці 2.5

Кроки			Документи	
№	Назва	Зміст робіт	Документ	Зміст документа
	Підготовка пакету авторизації СБІ	Пакет авторизації готує Власник/ Розпорядник ІС, який включає в нього: розроблений цільовий профіль безпеки ІС, звіт оцінювача, установчі документи організації, копії наявних ліцензій (в разі необхідності). Якщо інформація, яка міститься у Пакеті авторизації є ІзОД, то Власник/ Розпорядник ІС має вжити заходи для збереження конфіденційності та цілісності ІзОД відповідно до діючого законодавства, в тому числі, із використанням заходів технічного захисту інформації	Пакет авторизації	Цільовий профіль безпеки Висновок оцінювача про правильність визначення цільового профілю Висновок оцінювача про відповідність СБІ цільовому профілю. Відомості про ІС Відомості про Власника/ Розпорядника ІС Копії ліцензій
	Авторизація СБІ	Прийняття рішення щодо можливості внесення ІС до реєстру авторизованих систем на основі аналізу пакету авторизації	Рішення уповноваженого органу з авторизації	Задокументоване рішення щодо внесення ІС в реєстр авторизованих систем.
		Внесення ІС в реєстр авторизованих систем	Запис в Реєстрі авторизованих ІС	Інформація про ІС у нормативно визначеному форматі
		Виявлення недоліків	Повідомлення від Уповноваженого органу з авторизації Власнику /Розпоряднику ІС	Перелік недоліків
Етап 6. Супроводження КСЗІ				

Наявність різних документів стосовно кіберзахисту вимагається на ОІД згідно з різними законодавчими актами (рис.2.3).

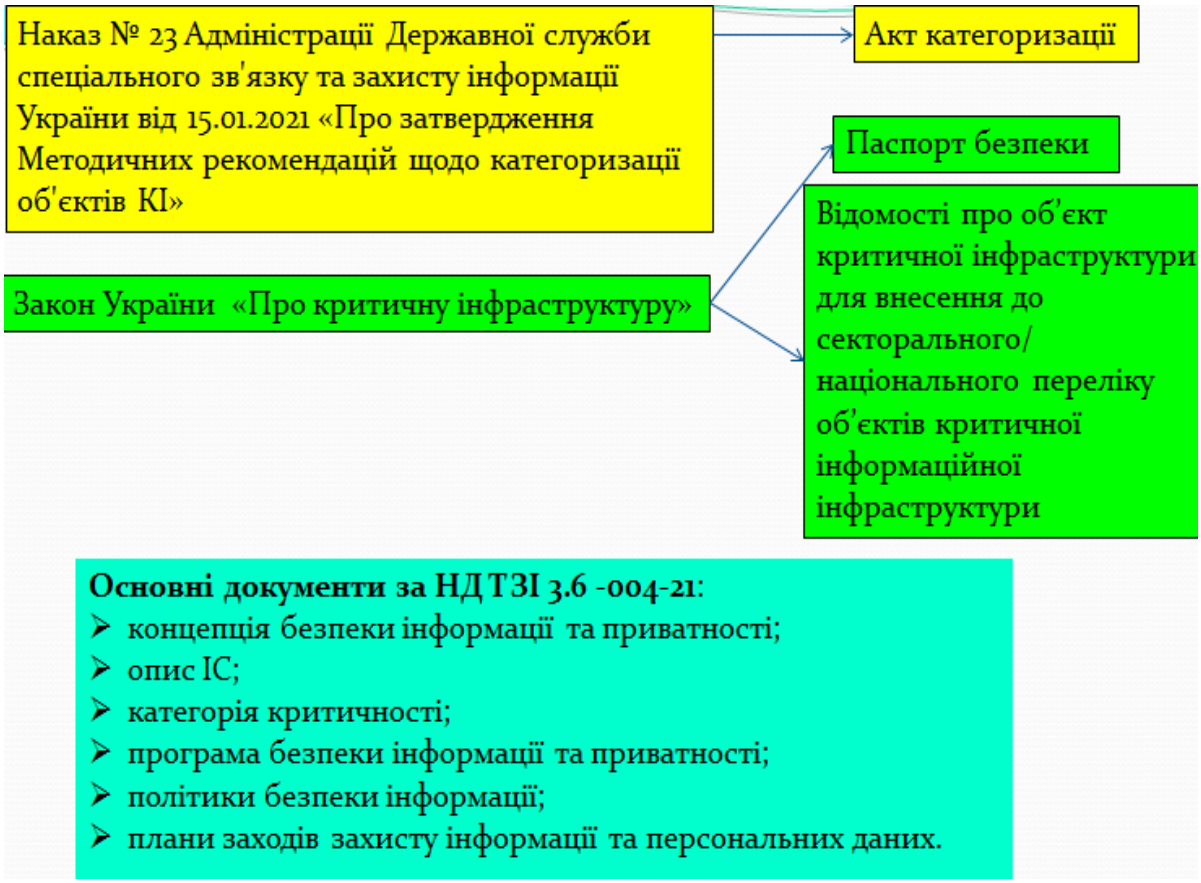


Рисунок 2.3 – Вимоги нормативних актів до складу документації

Основні документи і їх рекомендовані розділи (рис.2.4) перелічені в НД ТЗІ 3.6-004-21 «Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці» [67] для випадку створення СБІ. При цьому рекомендовані НД ТЗІ [67] розділи цих документів можуть доповнюватися на розсуд Власника або Розпорядника організації та/або ІС з метою врахування особливостей організації, особливостей ІС, нормативних вимог, сформованих центральними або галузевими органами влади. Сам перелік документів також може бути за потребою доповнений.

Назва документу	Рекомендовані розділи
Концепція БІ (Організаційний рівень)	1. Висновки щодо явного прийняття ризиків на рівні вищого керівництва. 2. Наміри керівництва. 3. Припущення , що будуть успадковуватися програмою безпеки інформації та приватності. 4. Виділення ІС у складі Організації. 5. Виділення структурних компонентів Організації.
Опис ІС (Системний рівень)	1. Опис організаційної належності ІС, 2. Опис процедур, функцій, активів, прикладних процесів ІС, 3. Опис дійових осіб ІС, 4. Варіанти використання ІС, 5. Результати інвентаризації ІТ-активів, 6. Результати інвентаризації типів інформації ІС
Категорія критичності ІС (Системний рівень)	1. Визначення рівнів критичності типів інформації в ІС 2. Визначення категорії критичності ІС
Програма безпеки інформації та приватності (Системний рівень)	1. Формулювання вимоги безпеки ІС 2. Формулювання вимоги приватності ІС 3. Обґрунтування вибору базового профілю безпеки або галузевого профілю безпеки 4. Обґрунтування вибору рівня базового профілю безпеки або галузевого профілю безпеки 5. Місце впровадження ІС в структурі Організації
Політика безпеки (Системний рівень)	1. Ціль/цілі політики безпеки інформації 2. Сфера застосування Політики безпеки 3. Ролі в ІС та сфери їх відповідальності 4. Перегляд Політики безпеки
Плани заходів захисту (Системний рівень)	1. Застосовані в ІС технічні, програмні та організаційні засоби для реалізації заходів захисту 2. Обґрунтування параметрів

Рисунок 2.4 - Рекомендовані НД ТЗІ 3.6-004-21 [67] розділи основних документів

3 РОЗРОБКА ШАБЛОНУ КСЗІ

3.1 Підхід до побудови КСЗІ на основі профілів безпеки

Згідно НД ТЗІ 3.7-003-2023 «Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем» [72] і моделлю впровадження системи безпеки інформації, яка проаналізована у п.2.1 даної кваліфікаційної роботи, КСЗІ може бути побудована з використанням базових профілів безпеки, і в цьому випадку процес створення КСЗІ має відповідати НД ТЗІ 3.6-004-21 «Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці» [67], а оцінка КСЗІ під час проведення державної експертизи - НД ТЗІ 2.3-025-21 «Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем» [63].

Профіль безпеки є набором заходів захисту, що застосовуються до інформації або до ІС. Розрізняють 4 типи взаємопов’язаних профілів безпеки:

− базовий – мінімальний набір заходів захисту для ІС певної категорії критичності, основа для створення галузевого і цільового профілів безпеки;

− галузевий – уточнений базовий профіль, який враховує особливості галузі;

− цільовий – уточнений базовий або галузевий профіль, який враховує вимоги чинних для даної ІС нормативно-правових актів і особливості конкретної ІС, такі як політик безпеки, призначення ІС, структурно-функціональні характеристики ІС, результати аналізу ризиків безпеки, особливості функціонування ІС;

– адаптований – профіль, що підлягає реалізації і утворюється на основі цільового профілю шляхом удосконалень заходів захисту, заміни (в разі можливості) заходів захисту, які обґрунтовано не можуть бути реалізовані в певній ІС, на еквівалентні за дією засоби захисту і виключення засобів захисту, які не можуть бути реалізовані в конкретній ІС і не мають еквівалентної заміни.

Впровадження СБІ складається з семи етапів (рис.3.1), на кожному з яких вирішується певний набір задач і оформлюються певні документи (див.рис.2.4).

Рисунок 3.1 – Етапи впровадження СБІ

На рис.3.1 виділена задача, автоматизації котрої присвячена практично частина даної кваліфікаційної роботи. На етапі вибору заходів захисту за результатами оцінки ризиків та категоріювання безпеки у порядку, визначеному НД ТЗІ 3.6-006-24 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної

таємниці, для інформаційних систем» [69] обирається базовий (галузевий) профіль безпеки у - набір заходів захисту.

СБІ має задовольняти вимогами безпеки, які визначаються для ІС, виходячи з нормативно-правової бази і потреб конкретної організації, і вимогам приватності, спрямованих на захист персональних даних приватних осіб. Вимоги безпеки та приватності, а також прийняті організацією ризики визначаються в Концепції безпеки інформації та приватності організації, для реалізації котрої складається Програма безпеки інформації та приватності.

У додатку А НД ТЗІ 3.6-006-24 [69] наведені три базових профілі безпеки для ІС низької, середньої та високої категорії критичності і заходи захисту персональних даних. Заходи захисту та посилення заходів захисту, які наявні в НД ТЗІ 3.6-006-24 [69], але не внесені в жоден базовий профіль безпеки, можуть бути обрані розробником галузевого або цільового профілю самостійно, якщо для ефективного реагування на виявлені ризики необхідно впроваджувати додаткові заходи захисту або посилення заходів захисту.

Наказом №317 Адміністрації Держспецзв'язку [57] у 2024 році були затверджені у оприлюднених частинах базові профілі безпеки для ІКС, де обробляється відкрита інформація, і для ІКС, де обробляється службова інформація.

3.2 Базові алгоритми

Вибір профілю безпеки, вибір засобів захисту СБІ в циклічній моделі Плануй-Виконуй-Перевіряй-Дій (ПВПД) і послідовність перетворення базового профілю безпеки в адаптований профіль здійснюється за алгоритмами, наведеними на рис.3.2-3.4.

Представлення базових профілів в НД ТЗІ 3.6-006-24 [69] (рис.3.5) і у Наказі №317 [57] (рис.3.6) мають ряд відмінностей, зокрема, в базових профілях, наведених в Наказі №317 [57] не виокремлені заходи захисту, призначені для задоволення вимог приватності.

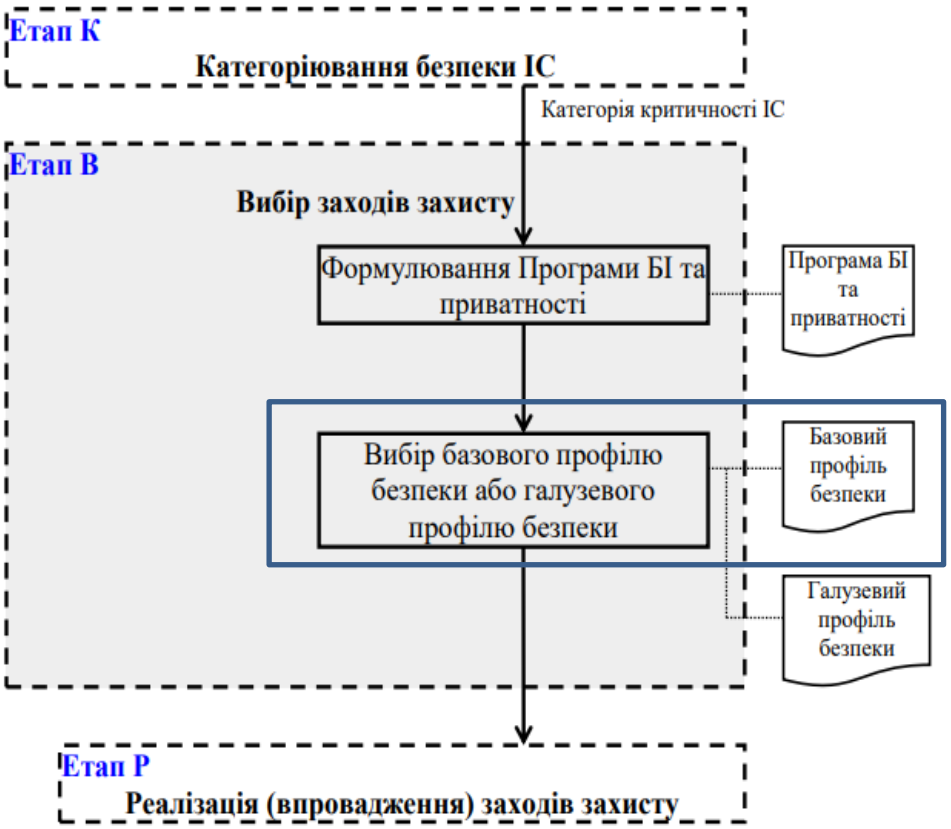


Рисунок 3.2 – Вибір профілю безпеки за НД ТЗІ 3.6-006-24 [69]

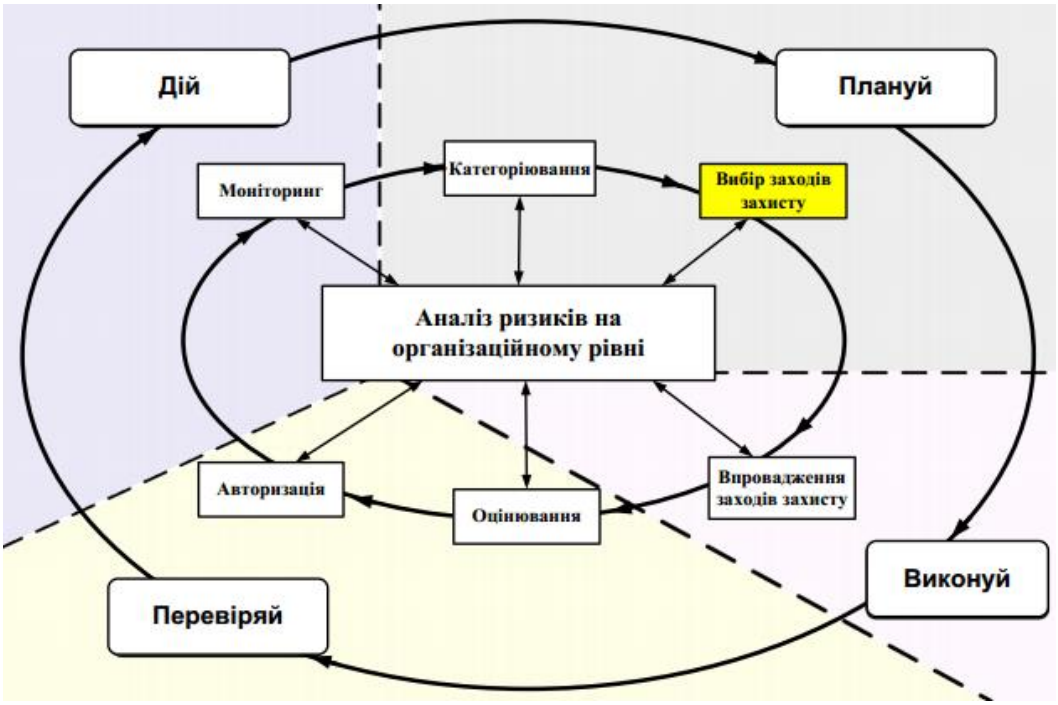


Рисунок 3.3 – Вибір засобів захисту СБІ в моделі ПВПД (ISO/IEC 27001 [42]) за НД ТЗІ 3.6-006-24 [69]

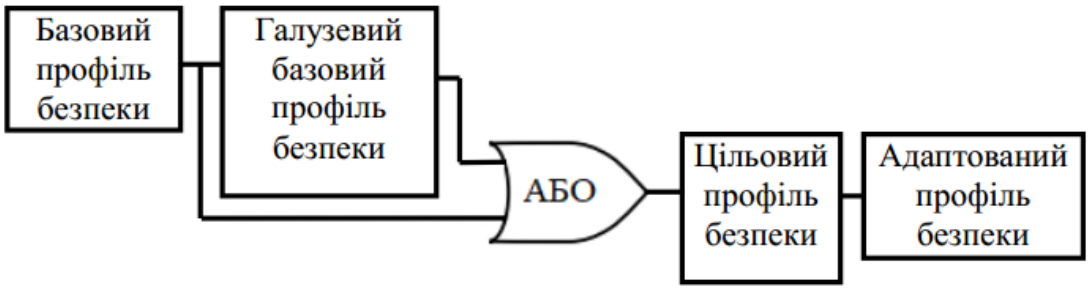


Рисунок 3.4 – Послідовність отримання профілів безпеки за НД ТЗІ 3.6-006-24 [69]

Шифр	Назва заходу захисту	Приват ність	Рівні безпеки		
			Низький	Середній	Високий
УПРАВЛІННЯ ДОСТУПОМ (AC)					
AC-1	Політика та процедури управління доступом	AC-1	AC-1	AC-1	AC-1
AC-2	Управління обліковими записами		AC-2	AC-2 (1) (2) (3) (4) (5) (13)	AC-2 (1) (2) (3) (4) (5) (11) (12)(13)
AC-3	Забезпечення доступу	AC-3 (14)	AC-3	AC-3	AC-3

Рисунок 3.5 – Представлення базових профілів безпеки в НД ТЗІ 3.6-006-24 [69]

Розділ I. Для інформаційно-комунікаційної системи, де обробляється відкрита інформація.

№	Назва вимоги з безпеки інформації	Зміст вимоги	Заходи захисту інформації відповідно до НД ТЗІ 3.6-006-24
1.	**Управління доступом**		**АС**
1.1.	Управління обліковими записами	1) визначити дозволені та заборонені типи облікових записів у системі; 2) створювати, активувати, змінювати, деактивувати та видаляти облікові записи із системи відповідно до політики, процедур, передумов і критеріїв організації; 3) визначити авторизованих користувачів	АС-2

Рисунок 3.6 – Представлення базових профілів безпеки в Наказі №317 [57]

Таблиці рис.3.5 і рис.3.6 не відповідають умовам нормалізації і не можуть бути безпосередньо введені в базу даних. Тому були окремо створені таблиці «Класи заходів захисту» (Номер класу, Назва, Ідентифікатор класу), «Вимоги з

безпеки інформації», «Заходи захисту» і «Посилення заходів захисту» (див рис.4.3), пов’язані зв’язками один-до-багатьох.

В разі необхідності додавання інформації у базовий профіль безпеки використовується наступний алгоритм:

Крок 1. Внесення нових записів у таблицю «Класи заходів захисту».

Крок 2. Внесення змін в таблицю «Заходи захисту»

Крок 3. Внесення змін в таблицю «Посилення заходів захисту»

Крок 4. Внесення змін в таблицю «Вимоги з безпеки інформації»

В разі необхідності видалення інформації зміни в таблиці вносяться у зворотному порядку.

3.3 Представлення в базі даних заходів захисту і базового профілю безпеки

Заходи захисту в каталозі НД ТЗІ 3.6-006-24 [69] закодовані і мають структуру, наведену на рис. 3.7

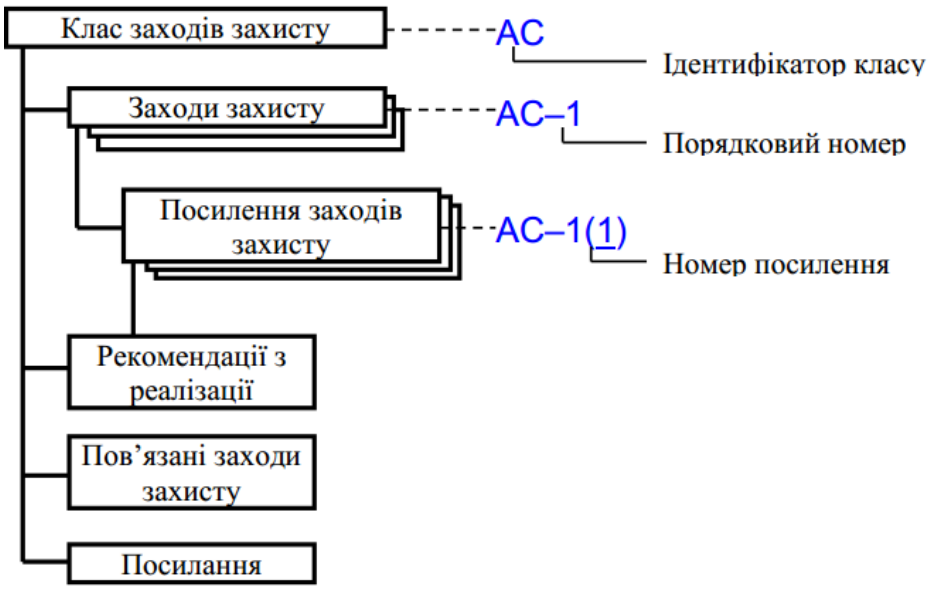


Рисунок 3.7 – Структура заходів захисту в каталозі НД ТЗІ 3.6-006-24 [69]

Кількість посилень, пов'язаних заходів захисту і посилань у різних заходів захисту різна, окремі заходи захисту взагалі не мають посилень.

Описи заходів захисту містять наступні змістові блоки (рис.3.8):

– «основний розділ;
– розділ рекомендацій з реалізації;
– розділ посилення заходу;
– розділ, який містить інформацію про пов'язані заходи захисту;
– довідковий розділ (посилання)» [69].

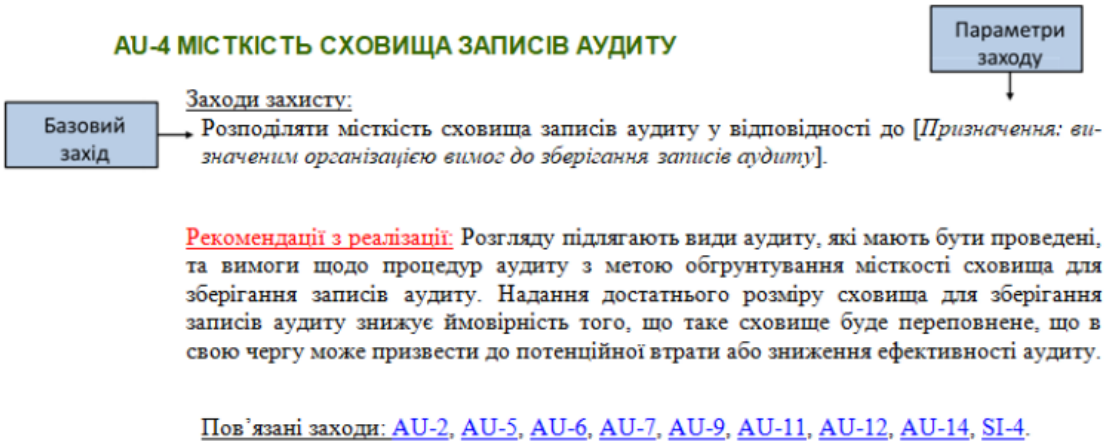


Рисунок 3.8 – Структура заходів захисту в каталозі НД ТЗІ 3.6-006-24 [69] на прикладі *AU*-4, що не має посилань

Таким чином, для кожного заходу захисту визначені:

– код класу заходів захисту (на рис.3.8 – *AU*);
– назва класу заходів захисту (для класу – «Аудит та підзвітність»);
– номер заходу захисту у класі (на рис.3.8 – 4);
– призначення заходу захисту (в розділі опису);
– параметри заходу захисту (в розділі опису);
– рекомендації з реалізації (текстовий блок, обсяг якого є різним для різних заходів. Тому при розробці бази даних в *MS Access* рекомендації з реалізації мають представлятися полем типу *MEMO*);
– кількість наявних посилень (в тому числі 0 в разі відсутності посилень), що визначається з розділу посилення заходу;

– перелік посилень (в разі їх наявності), наведений в розділі посилення заходу;

– кількість пов’язаних заходів захисту (в тому числі 0 в разі відсутності пов’язаних із даним заходів захисту), що визначається з відповідного розділу;

– перелік пов’язаних заходів захисту (в разі їх наявності), наведений у відповідному розділі;

– кількість посилань (в тому числі 0 в разі відсутності посилань), що визначається з довідникового розділу;

– перелік посилань (в разі їх наявності), наведений у довідниковому розділі.

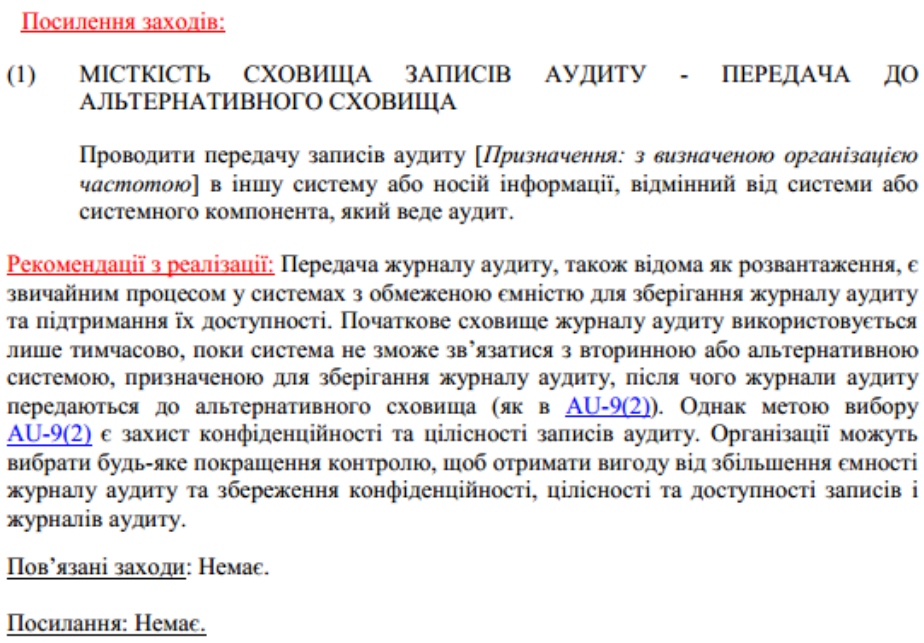
Описи посилень заходів захисту мають аналогічну структуру (за виключенням розділу посилення заходу) (рис.3.9):

– основний розділ;

– розділ рекомендацій з реалізації;

– розділ, який містить інформацію про пов’язані заходи захисту;

– довідковий розділ (посилання) [69].



Посилення заходів:

(1) МІСТКІСТЬ СХОВИЩА ЗАПИСІВ АУДИТУ - ПЕРЕДАЧА ДО АЛЬТЕРНАТИВНОГО СХОВИЩА

Проводити передачу записів аудиту [*Призначення: з визначеною організацією частотою*] в іншу систему або носій інформації, відмінний від системи або системного компонента, який веде аудит.

Рекомендації з реалізації: Передача журналу аудиту, також відома як розвантаження, є звичайним процесом у системах з обмеженою ємністю для зберігання журналу аудиту та підтримання їх доступності. Початкове сховище журналу аудиту використовується лише тимчасово, поки система не зможе зв’язатися з вторинною або альтернативною системою, призначеною для зберігання журналу аудиту, після чого журнали аудиту передаються до альтернативного сховища (як в AU-9(2)). Однак метою вибору AU-9(2) є захист конфіденційності та цілісності записів аудиту. Організації можуть вибрати будь-яке покращення контролю, щоб отримати вигоду від збільшення ємності журналу аудиту та збереження конфіденційності, цілісності та доступності записів і журналів аудиту.

Пов’язані заходи: Немає.

Посилання: Немає.

Рисунок 3.9 – Структура посилень заходів захисту в каталозі НД ТЗІ 3.6-006-24 [69] на прикладі *AU*-4(1)

4 АПРОБАЦІЯ РОЗРОБКИ

4.1 Загальна характеристика бази даних

Для апробації алгоритмів визначення заходів захисту відповідно до базового профілю безпеки (рис.3.2, 3.3) було розроблено базу даних в MS Access, яка дозволяє користувачу:

а) отримувати інформаційну підтримку в процесі визначення заходів захисту, що відповідають базовому профілю безпеки, за рахунок наявної в базі бібліотеки нормативно-правових актів. Користувачі мають можливість:

− ознайомитися з оригіналами документів;

− здійснити вибірку документів за параметрами, передбаченими системою розроблених запитів;

− отримати звіти за результатами запитів у стандартизованому вигляді;

− в разі потреби самостійно формувати необхідні запити і звіти, а також змінювати значення атрибутів документів (наприклад, "чинний" на "втратив чинність") і додавати в базу нову інформацію;

б) визначати заходи захисту, що відповідають базовому профілю безпеки відповідно до НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем» [69] і Наказу Адміністрації Держспецзв’язку від 24.06.2024 № 317 «Про визначення Базового профілю безпеки інформації» [57], зокрема:

− робити вибірки заходів захисту і їх посилень;

− визначати пов'язані заходи захисту;

− визначати посилання заходів захисту;

− визначати вимоги з безпеки інформації, що відповідають базовому профілю безпеки.

Розроблена база даних:

− не містить інформації обмеженого доступу.

– забезпечує цілісність наявної в ній інформації;

– не передбачає в поточній версії будь-яких обмежень прав користувачів;

– є вільнорозповсюджуваною.

4.2 Структура бази даних

До складу розробленої бази даних входять таблиці, форми, запити і звіти. Склад таблиць і форм бази даних наведено на рис.4.1.

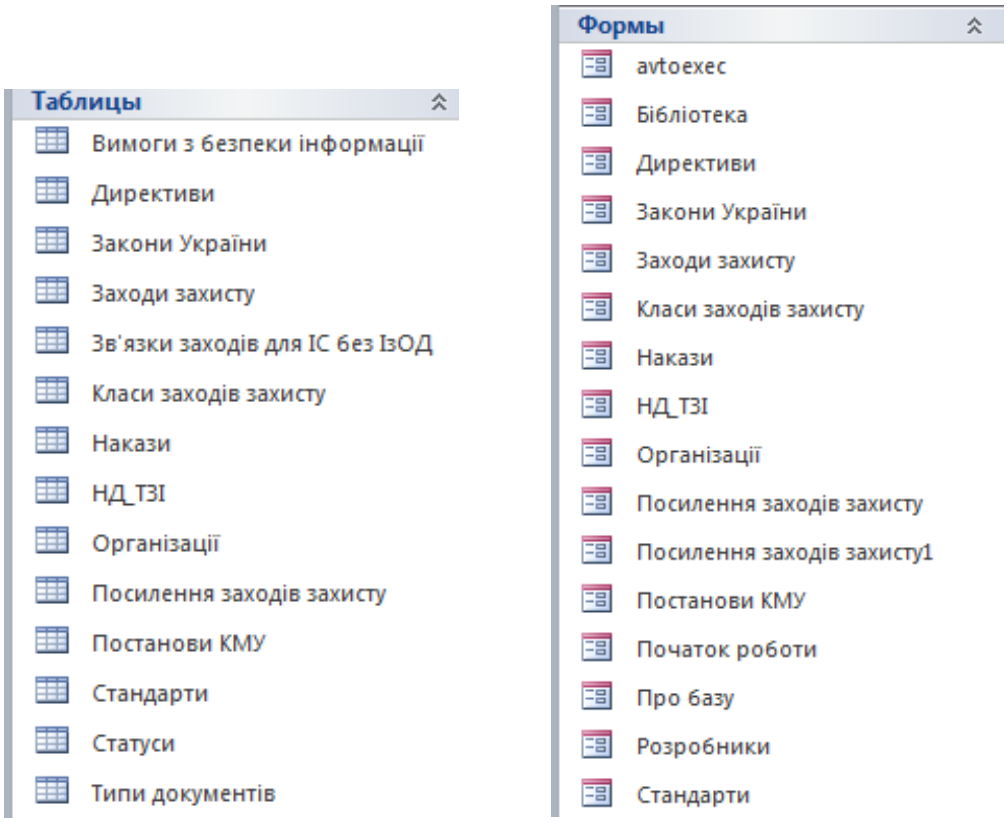


Рисунок 4.1 – Склад таблиць і форм бази даних

Серед таблиць бази даних наявні:

– таблиці, створені для підстановок: «Типи документів», «Статуси»;

– таблиці блоку інформаційної підтримки: «Директиви», «Закони України», «Накази», «Організації», «Постанови КМУ», «Стандарти»;

– таблиці блоку базового профілю безпеки: «Вимоги з безпеки інформації», «Класи заходів захисту», «Посилення заходів захисту», «Зв’язки заходів для ІС без ІзОД».

Схема бази даних містить два окремих блоки – рис.4.2 для бібліотеки нормативних документів і рис.4.3 для роботи з базовим профілем безпеки.

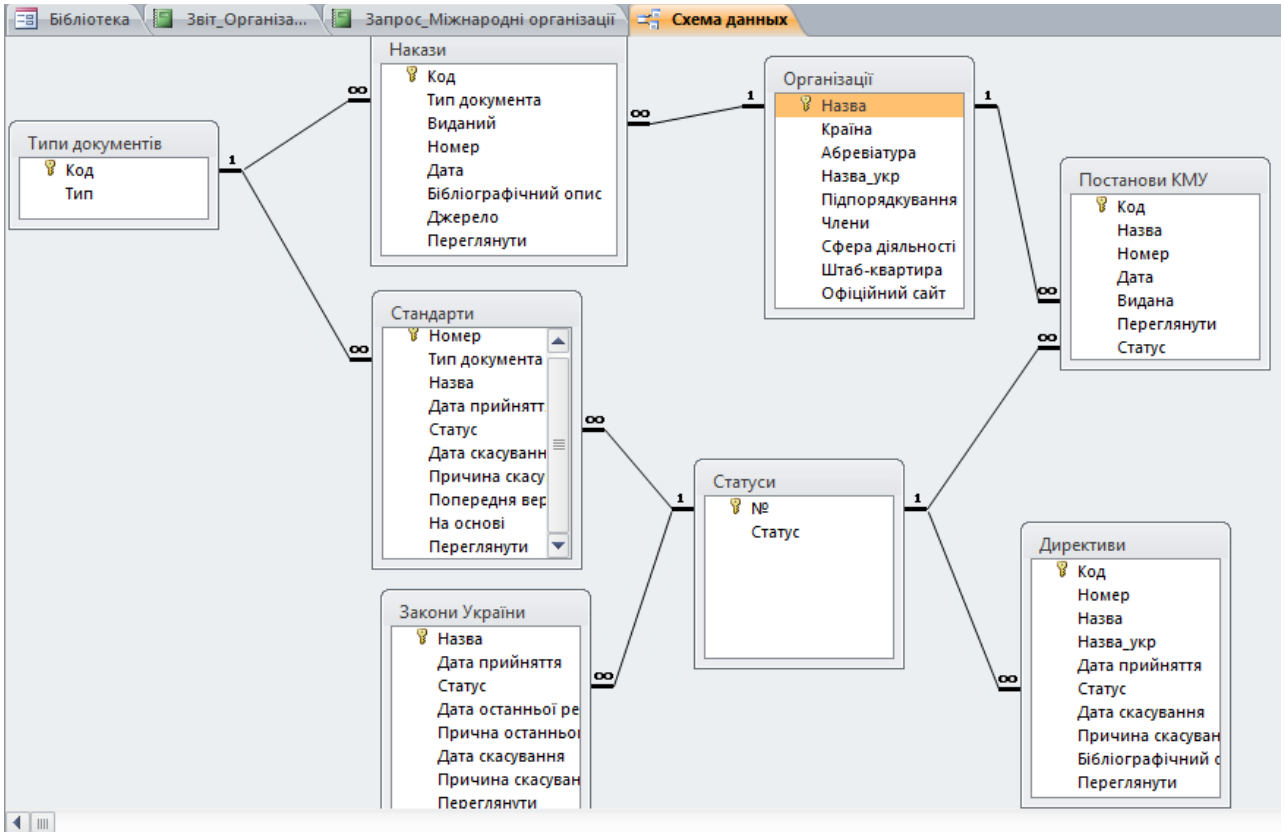


Рисунок 4.2 – Схема даних блоку інформаційної підтримки

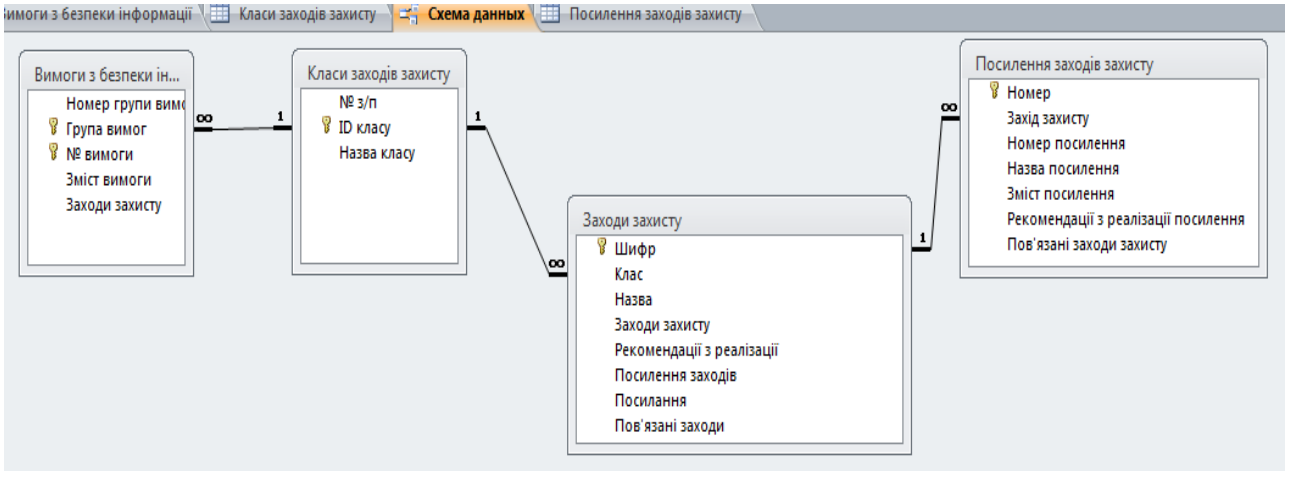


Рисунок 4.3 – Схема даних блоку роботи з базовим профілем безпеки

4.3 Початок роботи з базою даних

При запуску розробленої бази даних автоматично відкривається титульна форма «autoexec», наведена на рис.4.4, на якій наявні кнопки «Про систему», «Про розробників», «Почати роботу» і «Вихід».

Рисунок 4.4 – Титульна форма

При натискання кнопок «Про систему», «Про розробників» і «Почати роботу» відповідно відкриваються форми:

– «Про базу», на якій наведена інформація про призначення і функціональні можливості розробленої бази даних, характеристики інформації, що міститься в базі даних, умови розповсюдження бази даних;

– «Розробники», на якій наведено відомості про кафедру, яка видала завдання на кваліфікаційну роботу, автора бази і керівника роботи;

– «Початок роботи», на якій знаходяться кнопки «Ознайомитися з бібліотекою», «Оновлення інформації в базі», «Отримати відомості щодо базового профілю безпеки» і «»Закрити».

4.4 Ознайомлення з бібліотекою

При натискання кнопки «Ознайомитися з бібліотекою» відкривається форма «Бібліотека», наведена на рис.4.5.

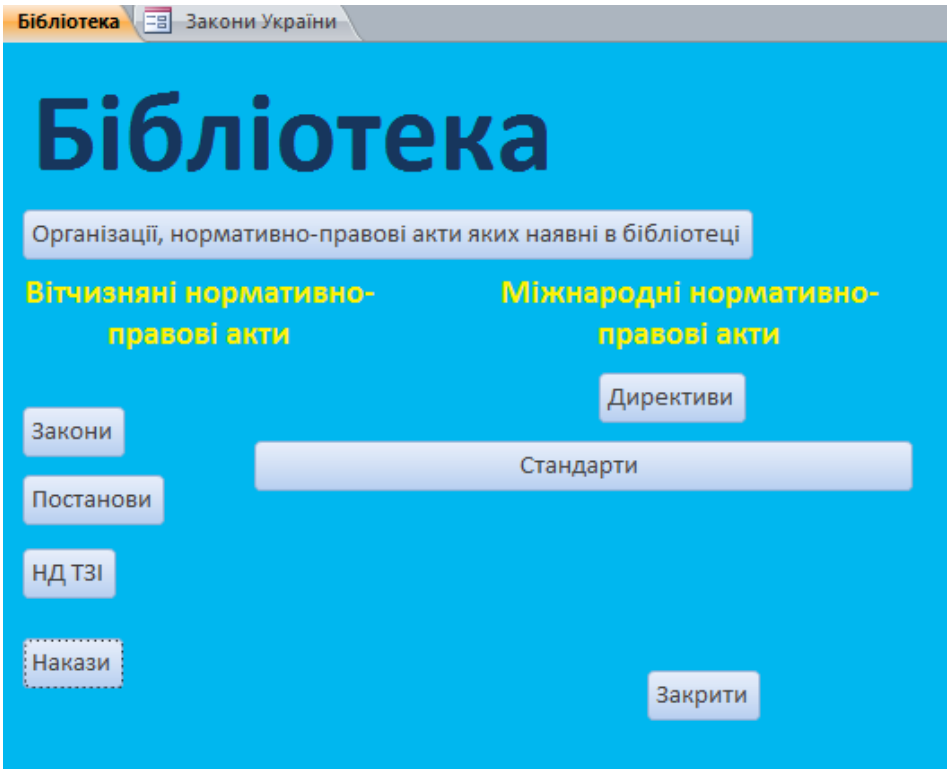


Рисунок 4.5 – Форма «Бібліотека»

На формі «Бібліотека»(рис.4.5) наявні кнопки для закриття цієї форми і перегляду вітчизняних і міжнародних нормативно-правових актів шляхом відкриття наступних форм:

– форма «Організації» (рис.4.6), яка містить відомості про організації, нормативно-правові акти котрих наявні в базі;

– форма «Закони» (рис.4.7), яка містить відомості про закони України, що стосуються тематики розробки;

– форма «Постанови КМУ» (рис.4.8), яка містить відомості про постанови Кабінету Міністрів України, що стосуються тематики розробки;

– форма «НД ТЗІ», яка містить відомості про нормативні документи з технічного захисту інформації (рис.4.9);

– форма «Директиви», яка містить відомості про директиви та інші документи Європейського Союзу (рис.4.10);

– форма «Стандарти», яка містить відомості про державні стандарти України і про міжнародні стандарти за тематикою розробки» (рис.4.11).

В усіх перелічених вище формах наявні гіперпосилання для перегляду занесених в базу нормативно-правових актів на офіційних сайтах організацій, що їх видали.

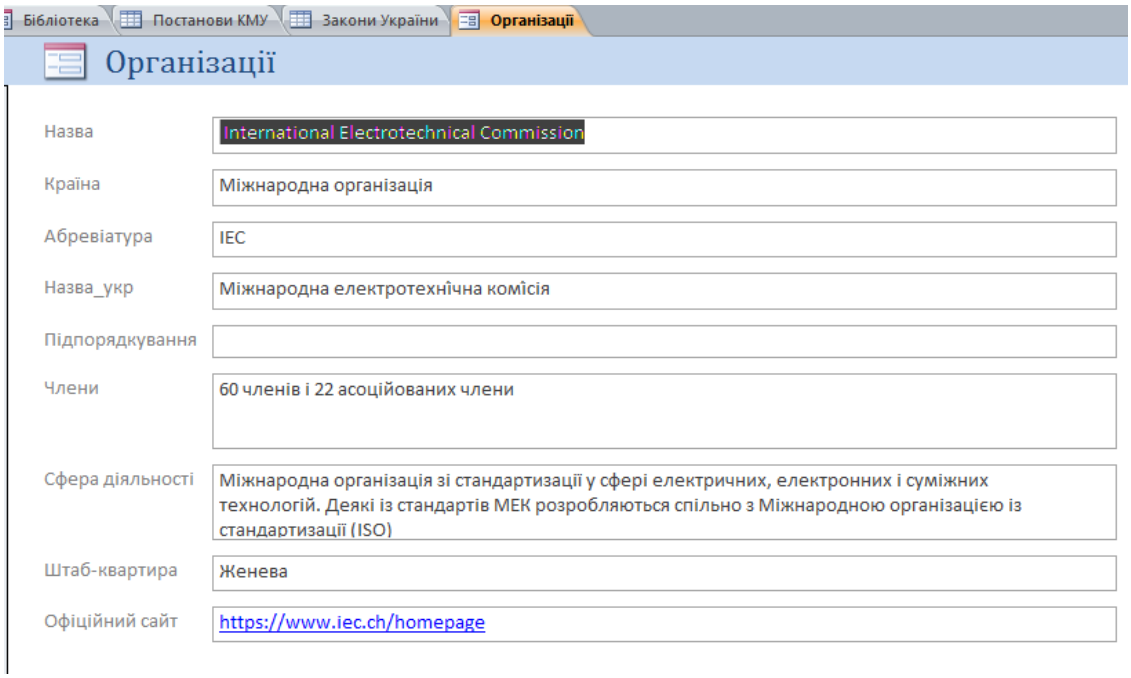


Рисунок 4.6 – Форма «Організації»

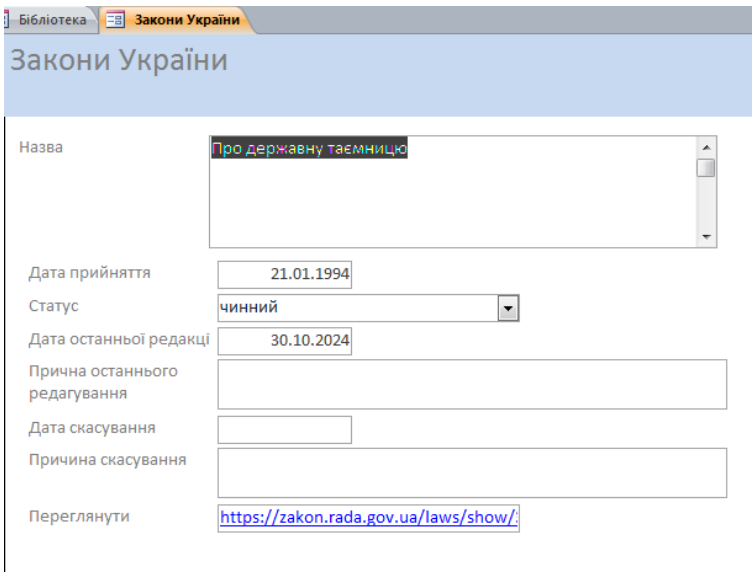


Рисунок 4.7 – Форма «Закони»

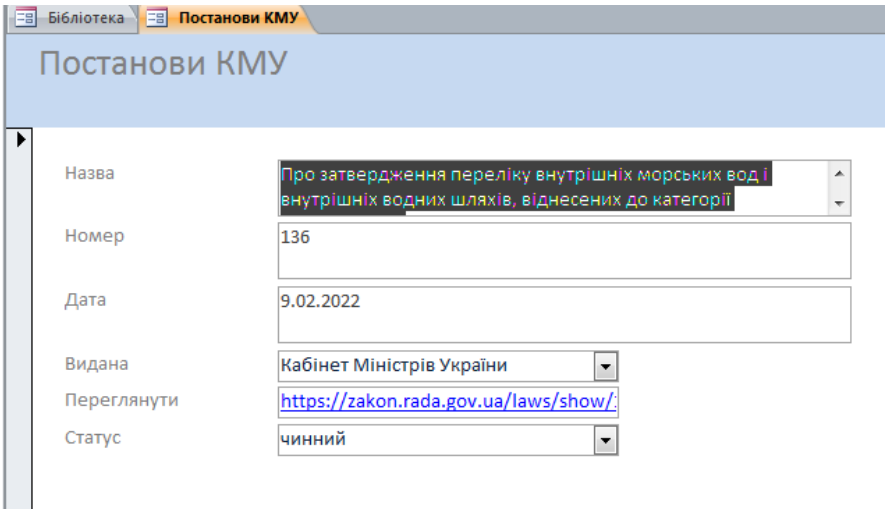


Рисунок 4.8 – Форма «Постанови КМУ»

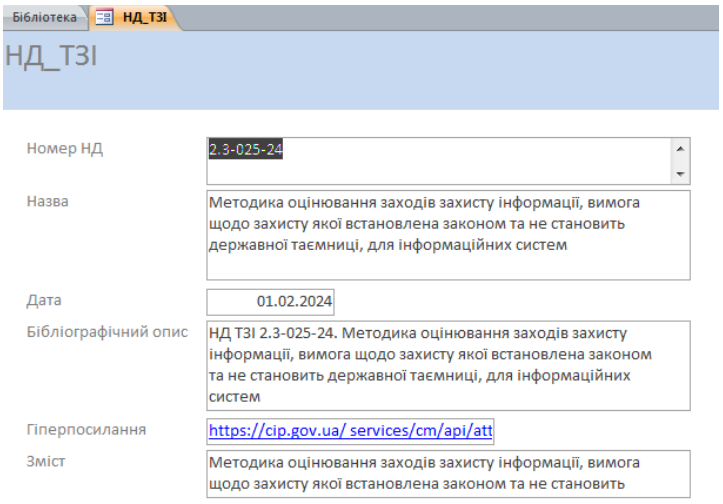


Рисунок 4.9– Форма «НД ТЗІ»

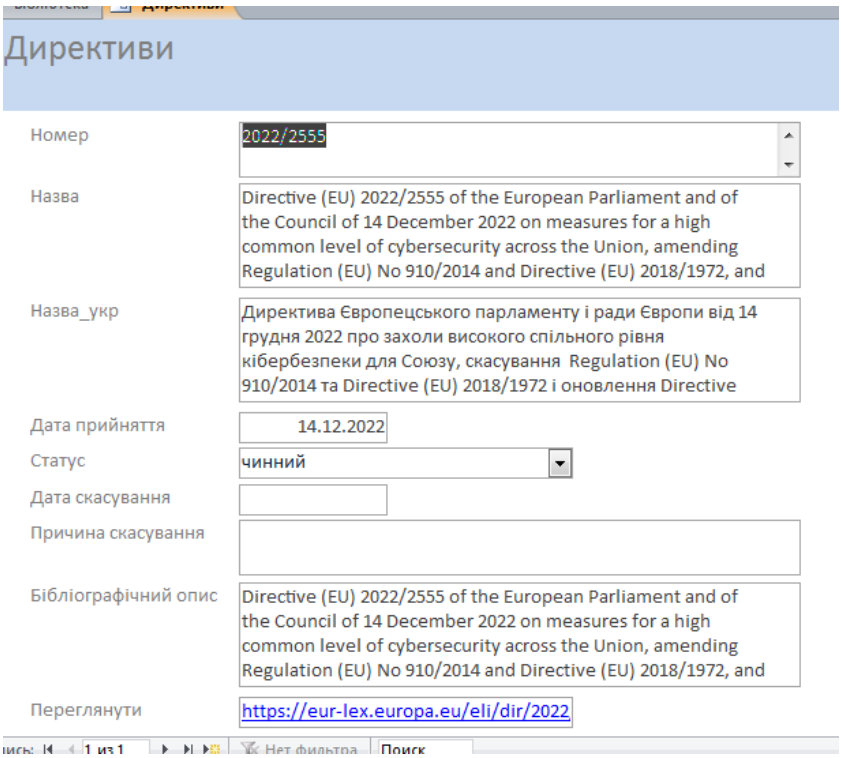


Рисунок 4.10 – Форма «Директиви»

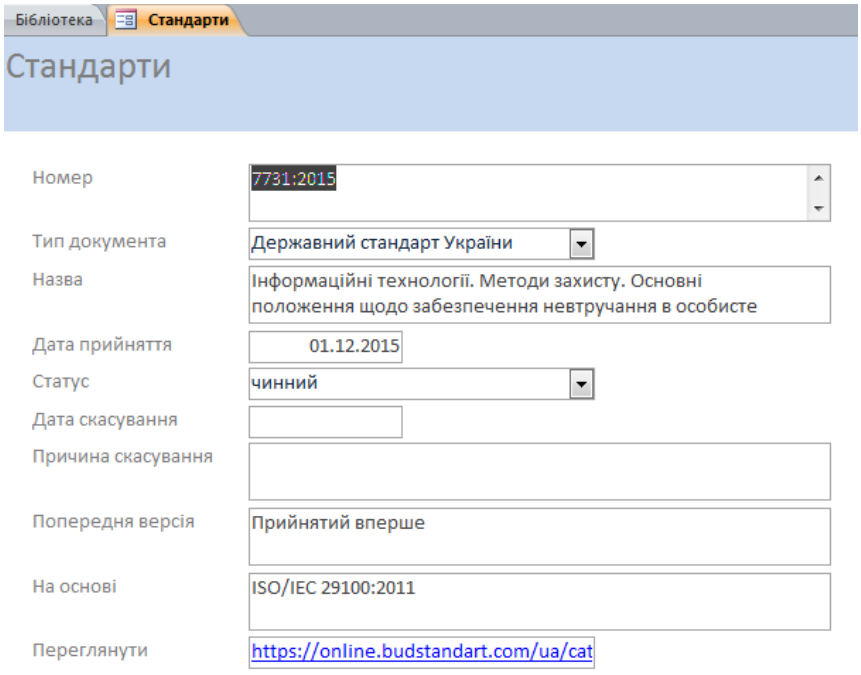


Рисунок 4.11 – Форма «Стандарти»

До кожної таблиці бази даних і до груп взаємопов’язаних таблиць можуть бути створені запити на вибірку за будь-яким атрибутом. Як приклад було створено запити до таблиці «Організації», які дозволяють переглянути сайти

вітчизняних (рис.4.12, 4.13) і міжнародних (рис.4.14, 4.15) організацій, які випускали будь-які нормативні акти за тематикою розробки.

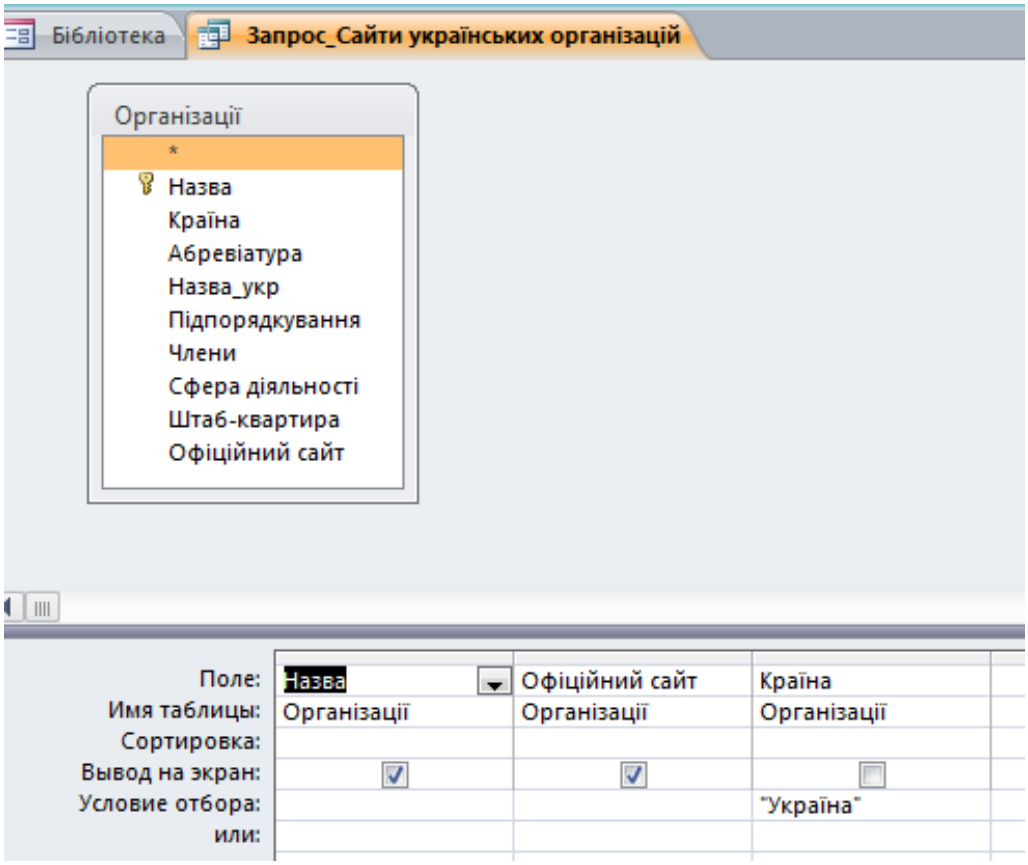


Рисунок 4.12 – Запит «Сайти українських організацій» в режимі конструктора в режимі конструктора

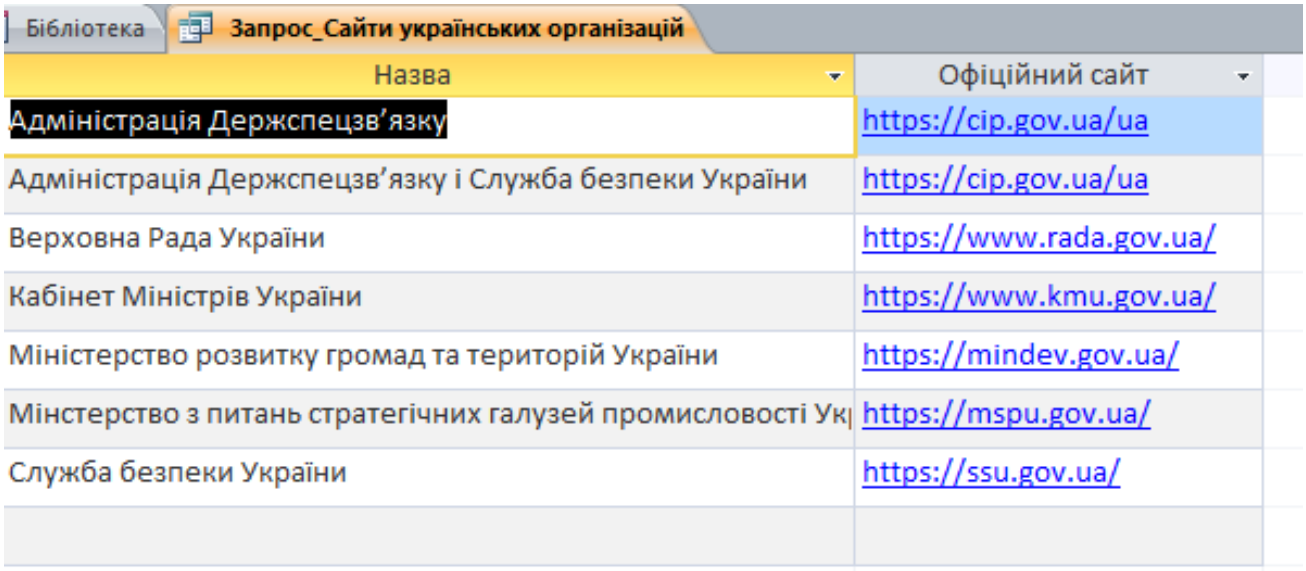


Рисунок 4.13 – Результат спрацьовування запиту «Сайти українських організацій»

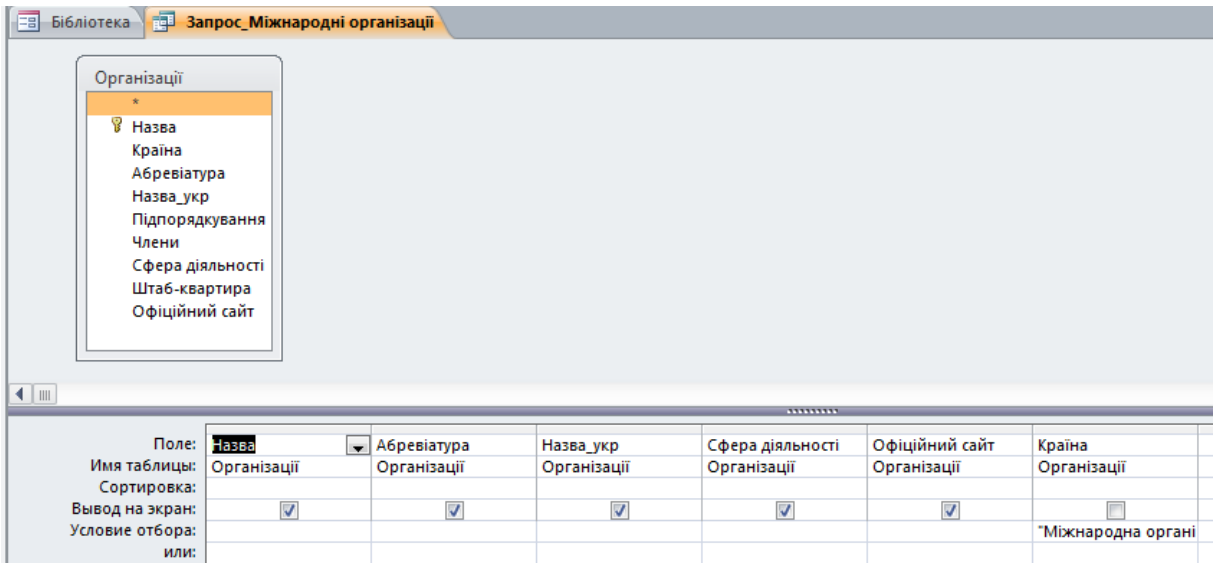
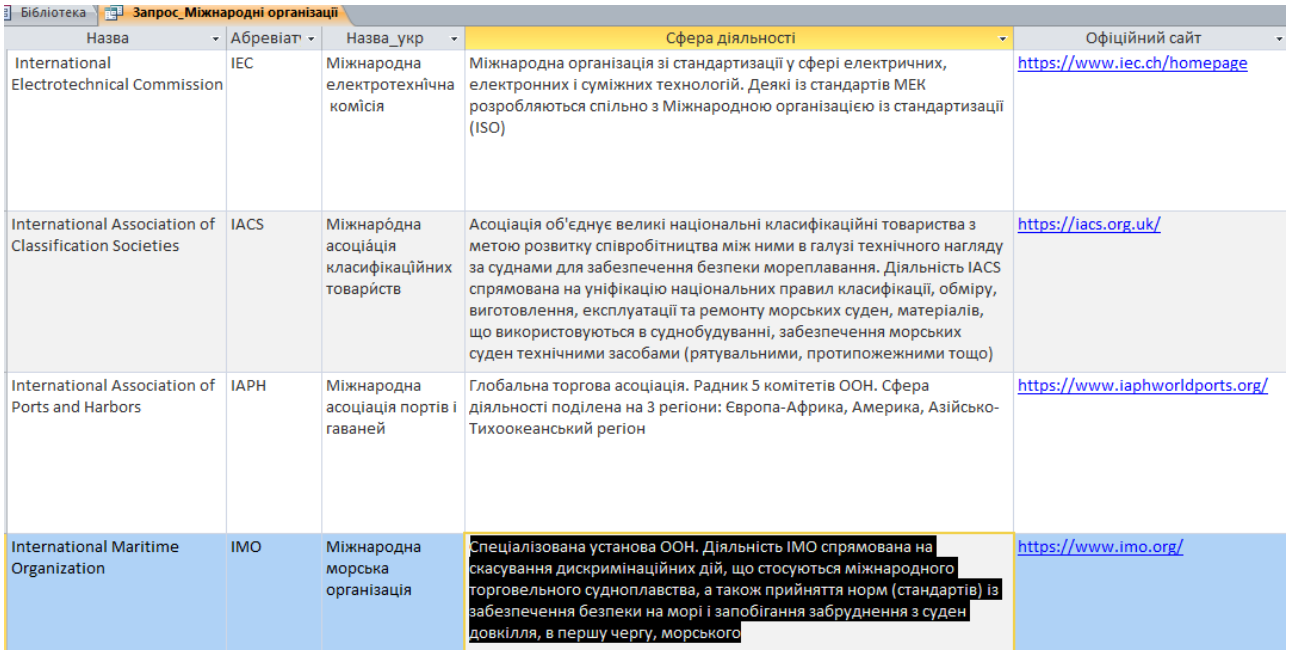


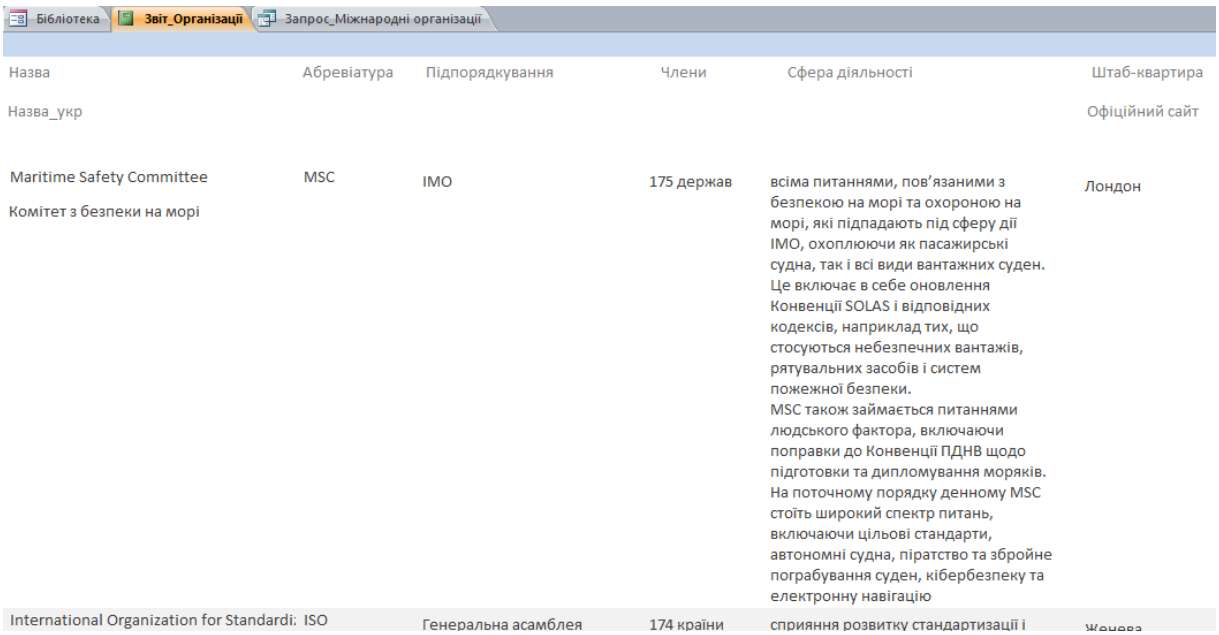
Рисунок 4.14 – Запит «Міжнародні організації» в режимі конструктора



Назва	Абревіат	Назва_укр	Сфера діяльності	Офіційний сайт
International Electrotechnical Commission	IEC	Міжнародна електротехнічна комісія	Міжнародна організація зі стандартизації у сфері електричних, електронних і суміжних технологій. Деякі із стандартів МЕК розробляються спільно з Міжнародною організацією із стандартизації (ISO)	https://www.iec.ch/homepage
International Association of Classification Societies	IACS	Міжнародна асоціація класифікаційних товариств	Асоціація об'єднує великі національні класифікаційні товариства з метою розвитку співробітництва між ними в галузі технічного нагляду за суднами для забезпечення безпеки мореплавання. Діяльність IACS спрямована на уніфікацію національних правил класифікації, обміру, виготовлення, експлуатації та ремонту морських суден, матеріалів, що використовуються в суднобудуванні, забезпечення морських суден технічними засобами (рятувальними, протипожежними тощо)	https://iacs.org.uk/
International Association of Ports and Harbors	IAPH	Міжнародна асоціація портів і гаваней	Глобальна торгова асоціація. Радник 5 комітетів ООН. Сфера діяльності поділена на 3 регіони: Європа-Африка, Америка, Азійсько-Тихоокеанський регіон	https://www.iaphworldports.org/
International Maritime Organization	IMO	Міжнародна морська організація	Спеціалізована установа ООН. Діяльність ІМО спрямована на скасування дискримінаційних дій, що стосуються міжнародного торговельного судноплавства, а також прийняття норм (стандартів) із забезпечення безпеки на морі і запобігання забруднення з суден довкілля, в першу чергу, морського	https://www.imo.org/

Рисунок 4.15 – Результат спрацьовування запиту «Міжнародні організації»

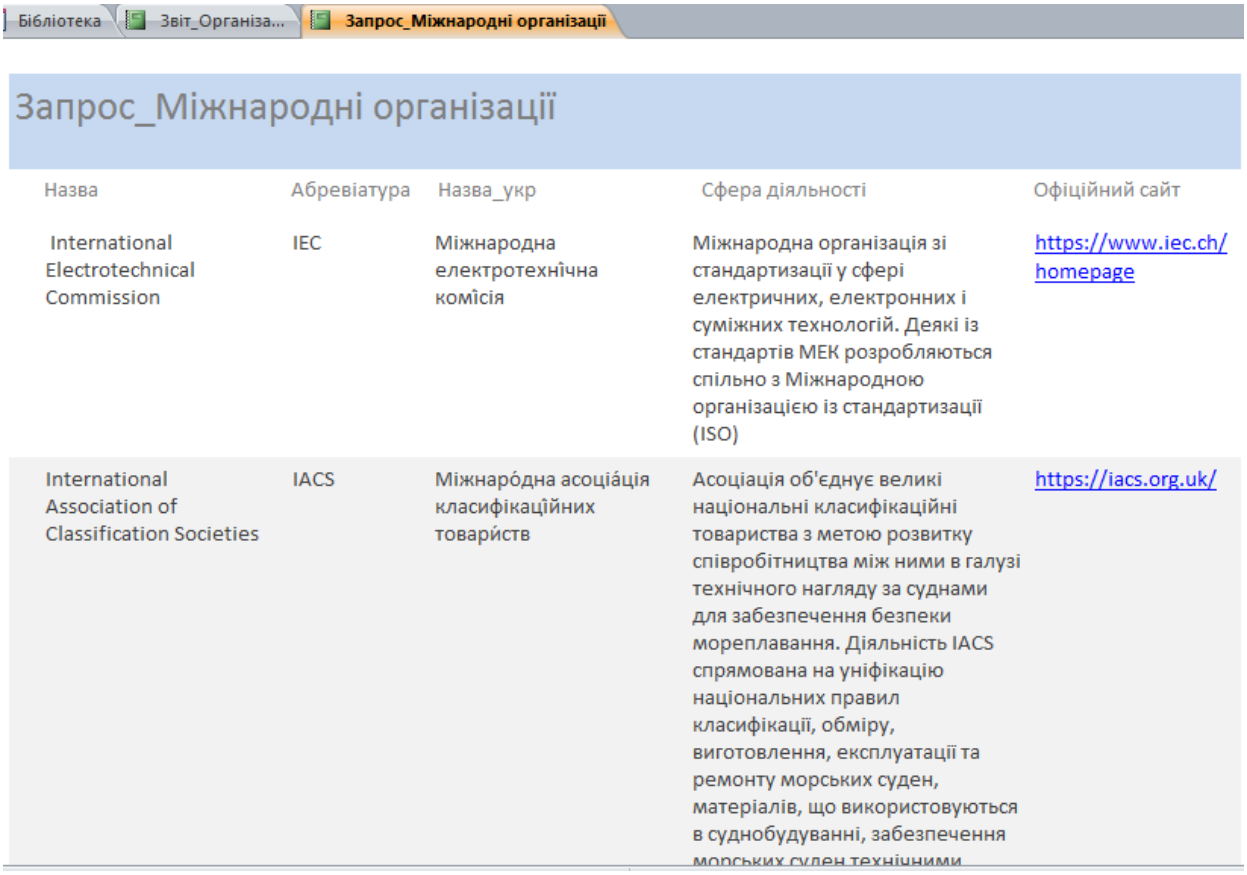
До кожної таблиці і результатів запиту може бути створений звіт. Оскільки права користувачів в даній версії бази не обмежуються, і база містить тільки відкриту інформацію, то користувачі можуть за допомогою конструктора або майстра звітів створювати і видавати на друк будь-які потрібні їм звіти. В якості прикладу були створені звіт за даними таблиці «Організації» (рис.4.16) і звіт за результатами спрацювання запиту «Міжнародні організації» (рис.4.17).



Бібліотека | Звіт_Організації | Запрос_Міжнародні організації

Назва Назва_укр	Абревіатура	Підпорядкування	Члени	Сфера діяльності	Штаб-квартира Офіційний сайт
Maritime Safety Committee Комітет з безпеки на морі	MSC	IMO	175 держав	всіма питаннями, пов'язаними з безпекою на морі та охороною на морі, які підпадають під сферу дії IMO, охоплюючи як пасажирські судна, так і всі види вантажних суден. Це включає в себе оновлення Конвенції SOLAS і відповідних кодексів, наприклад тих, що стосуються небезпечних вантажів, рятувальних засобів і систем пожежної безпеки. MSC також займається питаннями людського фактора, включаючи поправки до Конвенції ПДНВ щодо підготовки та дипломування моряків. На поточному порядку денному MSC стоїть широкий спектр питань, включаючи цільові стандарти, автономні судна, піратство та збройне пограбування суден, кібербезпеку та електронну навігацію	Лондон
International Organization for Standardi: ISO		Генеральна асамблея	174 країни	сприяння розвитку стандартизації і	Женева

Рисунок 4.16 – Звіт за даними таблиці «Організації»



Бібліотека | Звіт_Організа... | Запрос_Міжнародні організації

Запрос_Міжнародні організації

Назва	Абревіатура	Назва_укр	Сфера діяльності	Офіційний сайт
International Electrotechnical Commission	IEC	Міжнародна електротехнічна комісія	Міжнародна організація зі стандартизації у сфері електричних, електронних і суміжних технологій. Деякі із стандартів МЕК розробляються спільно з Міжнародною організацією із стандартизації (ISO)	https://www.iec.ch/homepage
International Association of Classification Societies	IACS	Міжнарóдна асоціáція класифікаційних товарúств	Асоціація об'єднує великі національні класифікаційні товариства з метою розвитку співробітництва між ними в галузі технічного нагляду за суднами для забезпечення безпеки мореплавання. Діяльність IACS спрямована на уніфікацію національних правил класифікації, обміру, виготовлення, експлуатації та ремонту морських суден, матеріалів, що використовуються в суднобудуванні, забезпечення морських суден технічними	https://iacs.org.uk/

Рисунок 4.17 – Звіт за результатами спрацювання запиту «Міжнародні організації»

4.5 Коригування інформації в базі даних

Таблиці бази даних можуть бути доповнені новими записами безпосередньо і режимі таблиці або через форму, створену для відповідної таблиці.

Слід мати на увазі, що таблиці, які спеціально створені для підстановок («Типи документів» рис.4.18, «Статуси» рис.4.19, «Організації» - рис.4.20), мають бути відредаговані в першу чергу.

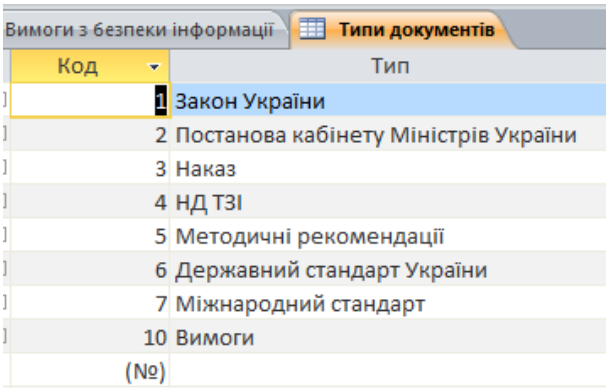


Рисунок 4.18 – Таблиця «Типи документів»

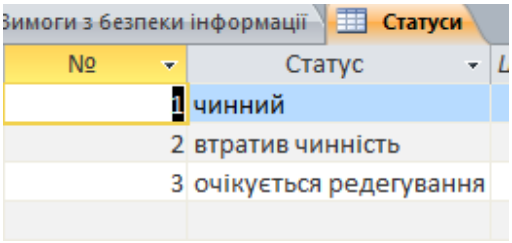


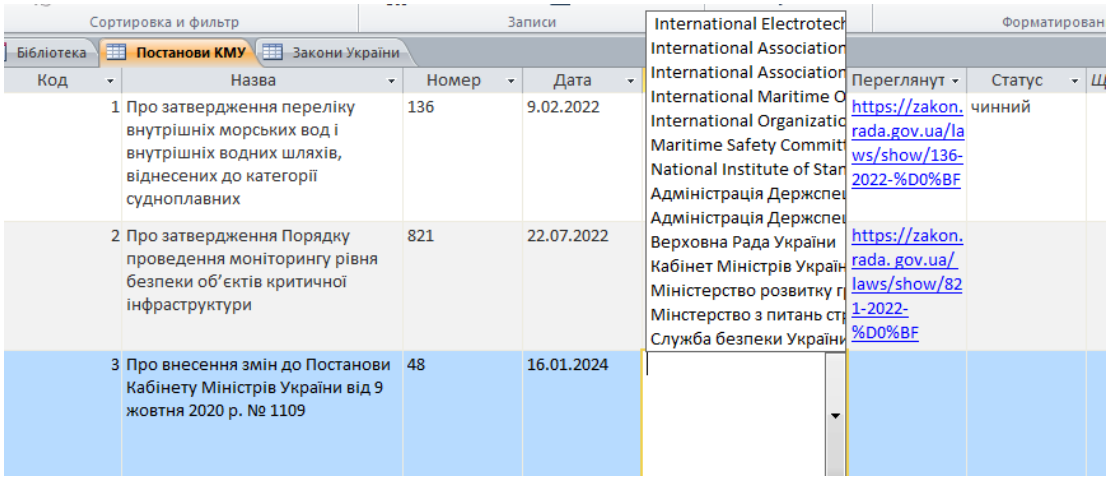
Рисунок 4.19 – Таблиця «Статуси»

Дані щодо організацій, які приймають участь у створенні нормативно-правового забезпечення кібербезпеки у галузі водного транспорту можуть бути змінені чи додані через форму «Організації» (рис.4.6).

Коригування складу класів заходів захисту, заходів захисту, посилень заходів захисту, вимог з безпеки інформації також може здійснюватися через відповідні таблиці або форми, враховуючи, що поля окремих таблиць використовуються для підстановок в інші таблиці (наприклад, рис.4.21).

Назва	Країна	Абревіатур	Назва_укр	Підпорядку	Члени	Сфера діяльності	Штаб-квартр	Офіційний сайт
International Electrotechnical Commission	Міжнародна організація	IEC	Міжнародна електротехнічна комісія		60 членів і 22 асоційованих члени	Міжнародна організація зі стандартизації у сфері електричних, електронних і суміжних технологій. Деякі із стандартів МЕК розробляються спільно з Міжнародною організацією із стандартизації (ISO)	Женева	https://www.iec.ch/homepage
International Association of Classification Societies	Міжнародна організація	IACS	Міжнародна асоціація класифікаційних товариств	Рада IACS	12 класифікаційних товариств	Асоціація об'єднує великі національні класифікаційні товариства з метою розвитку співробітництва між ними в галузі технічного нагляду за суднами для забезпечення безпеки мореплавання. Діяльність IACS спрямована на уніфікацію національних правил класифікації, обміру, виготовлення, експлуатації та ремонту морських суден, матеріалів, що використовуються в суднобудуванні, забезпечення морських суден технічними засобами (рятувальними, протипожежними тощо)	Лондон	https://iacs.org.uk/
International Association of Ports and Harbors	Міжнародна організація	IAPH	Міжнародна асоціація портів і гаваней	Секретаріат	більше 200 портів і національні представництва	Глобальна торгова асоціація. Радник 5 комітетів ООН. Сфера діяльності поділена на 3 регіони: Європа-Африка, Америка, Азійсько-Тихоокеанський регіон	Токіо	https://www.iaphworldports.org/
International Maritime Organization	Міжнародна організація	IMO	Міжнародна морська організація	ООН	175 держав	Спеціалізована установа ООН. Діяльність IMO спрямована на скасування дискримінаційних дій, що стосуються міжнародного торговельного судноплавства, а також прийняття норм (стандартів) із забезпечення безпеки на морі і запобігання забрудненню з суден довкілля, в першу чергу, морського	Лондон	https://www.imo.org/
International Organization for Standardization	Міжнародна організація	ISO	Міжнародна організація зі стандартизації	Генеральна асамблея	174 країни	сприяння розвитку стандартизації і суміжних видів діяльності у світі з метою забезпечення міжнародного обміну товарами і послугами, а також розвиток співробітництва в інтелектуальній, науково-технічній і економічній галузях	Женева	https://www.iso.org/ru/home.html
Maritime Safety	Міжнародна	MSC	Комітет з	IMO	175 держав	всіма питаннями, пов'язаними з безпекою на морі та охороною на морі, які підпадають під сферу дії IMO,	Лондон	

Рисунок 4.20 – Таблиця «Організації»



Сортировка и фильтр | Записи | Форматирован

Бібліотека | Постанови КМУ | Закони України

Код	Назва	Номер	Дата	Переглянут	Статус
1	Про затвердження переліку внутрішніх морських вод і внутрішніх водних шляхів, віднесених до категорії судноплавних	136	9.02.2022	https://zakon.rada.gov.ua/laws/show/136-2022-%D0%BF	чинний
2	Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури	821	22.07.2022	https://zakon.rada.gov.ua/laws/show/821-2022-%D0%BF	
3	Про внесення змін до Постанови Кабінету Міністрів України від 9 жовтня 2020 р. № 1109	48	16.01.2024		

International Electrotech
International Association
International Association
International Maritime O
International Organizatio
Maritime Safety Committ
National Institute of Stan
Адміністрація Держспец
Адміністрація Держспец
Верховна Рада України
Кабінет Міністрів Україн
Міністерство розвитку г
Мінстерство з питань ст
Служба безпеки України

Рисунок 4.21 – Таблиця «Постанови» в процесі заповнення

4.6 Робота з базовим профілем безпеки

Інформація в нормативних документах, що є базовими для даної кваліфікаційної роботи [57, 69] наведена у частково структурованому вигляді (рис.4.22).

Таблиця 9.1 — Перелік заходів захисту

Шифр	Назва
	УПРАВЛІННЯ ДОСТУПОМ (AC)
AC-1	Політика та процедури управління доступом
AC-2	Управління обліковими записами
AC-3	Забезпечення доступу
AC-4	Управління інформаційними потоками
AC-5	Розмежування обов'язків
AC-6	Мінімізація повноважень
AC-7	Невдалі спроби входу в систему
AC-8	Попередження про використання системи

Додаток
до наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України
___ _____ 2024 року № ___

Базовий профіль безпеки інформації

Розділ I. Для інформаційно-комунікаційної системи, де обробляється відкрита інформація.

№	Назва вимоги з безпеки інформації	Зміст вимоги	Заходи захисту інформації відповідно до НД ТЗІ 3.6-006-24
1.	**Управління доступом**		**АС**
1.1.	Управління обліковими записами	1) визначити дозволені та заборонені типи облікових записів у системі; 2) створювати, активувати, змінювати, деактивувати та видаляти облікові записи із системи відповідно до політики, процедур, передумов і критеріїв організації;	АС-2

10.1 Клас заходів захисту АС — УПРАВЛІННЯ ДОСТУПОМ

АС-1 ПОЛІТИКА ТА ПРОЦЕДУРИ УПРАВЛІННЯ ДОСТУПОМ

Заходи захисту:

a. Розробити, задокументувати та поширити [*Призначення: серед визначеного організацією персоналу або ролей*]:

1. [*Вибір (один або декілька): Рівень організації; Рівень місії/бізнес-процесу; рівень системи*] політики контролю доступу, яка:

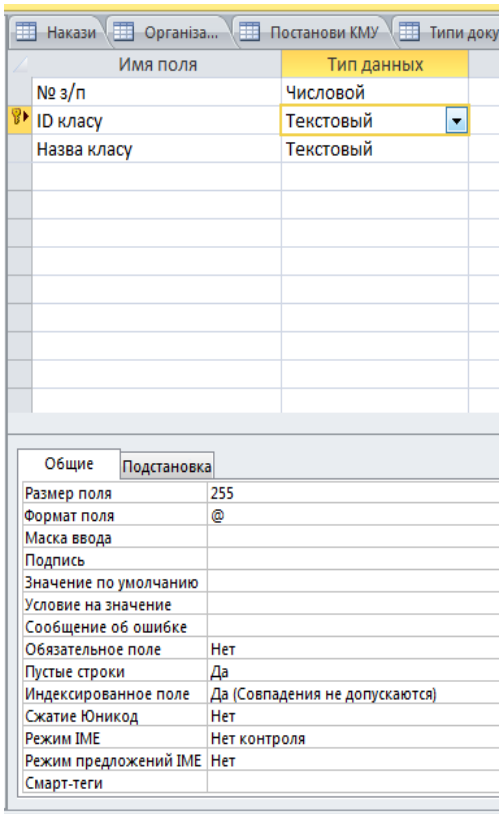
(a) містить мету, сферу застосування, ролі, відповідальність, зобов'язання керівництва, координацію між організаційними підрозділами та

Рисунок 4.22 – Представлення інформації в нормативних документах

Інформація в розробленій базі даних є структурованою повністю.

На рис.4.23 наведена таблиця «Класи заходів захисту» в режимі конструктора і в режимі таблиці (таблиця заповнена, на поточний момент наявні 20 класів згідно НД ТЗІ 3.6-006-21 [69] і Наказу Адміністрації Держспецзв'язку від 24.06.2024 № 317 [57]). Враховуючи, що номенклатура класів заходів захисту в подальшому може змінюватися для зручності внесення змін було створено форму рис.4.24.

а) режим конструктора



б) режим таблиці

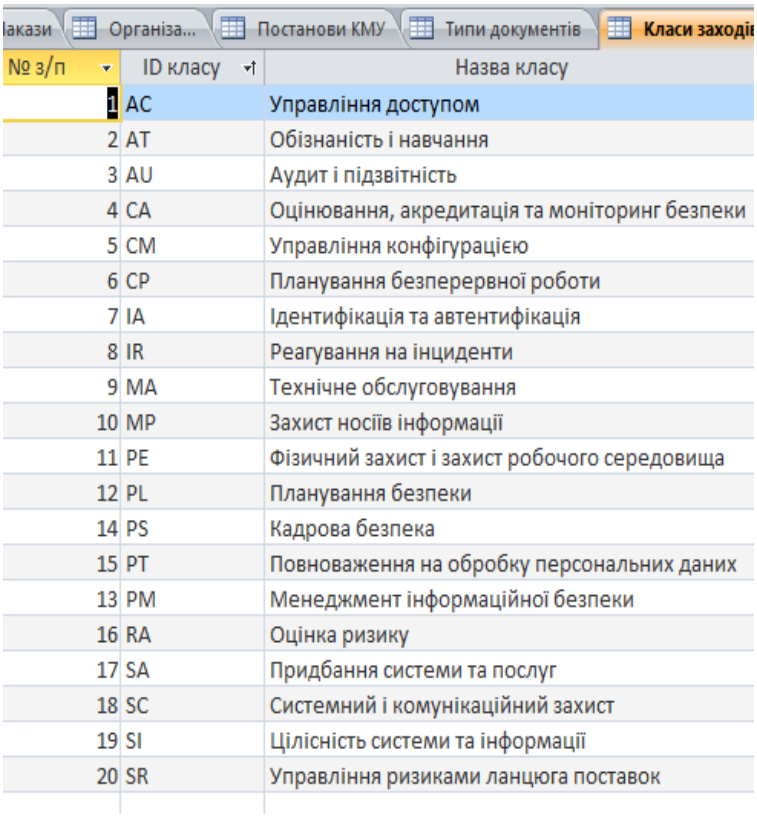


Рисунок 4.23 – Таблиця «Класи заходів захисту»

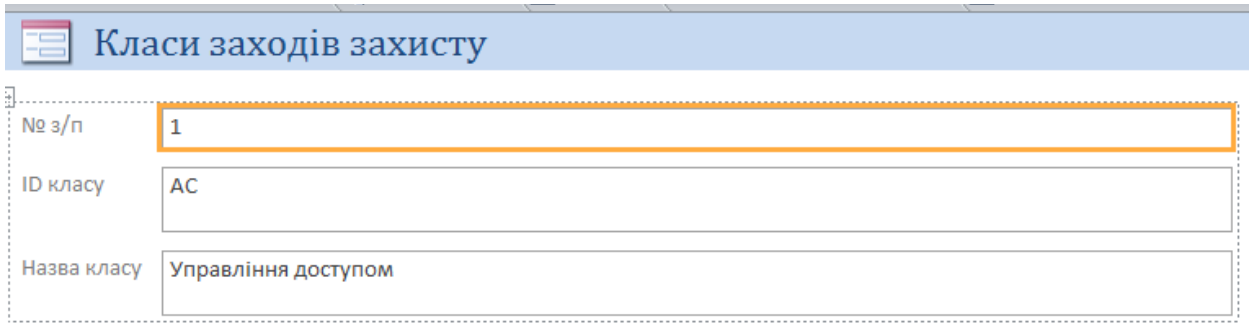


Рисунок 4.24 – Форма «Класи заходів захисту»

Заходи захисту представлені в таблиці «Заходи захисту» (рис.4.25), за якою була створена відповідна форма (рис.4.26)

Имя поля	Тип данных
Шифр	Текстовый
Клас	Текстовый
Назва	Текстовый
Заходи захисту	Поле MEMO
Рекомендації з реалізації	Поле MEMO
Посилення заходів	Поле MEMO
Посилання	Текстовый
Пов'язані заходи	Текстовый

Рисунок 4.25 – Таблиця «Заходи захисту» в режимі конструктора

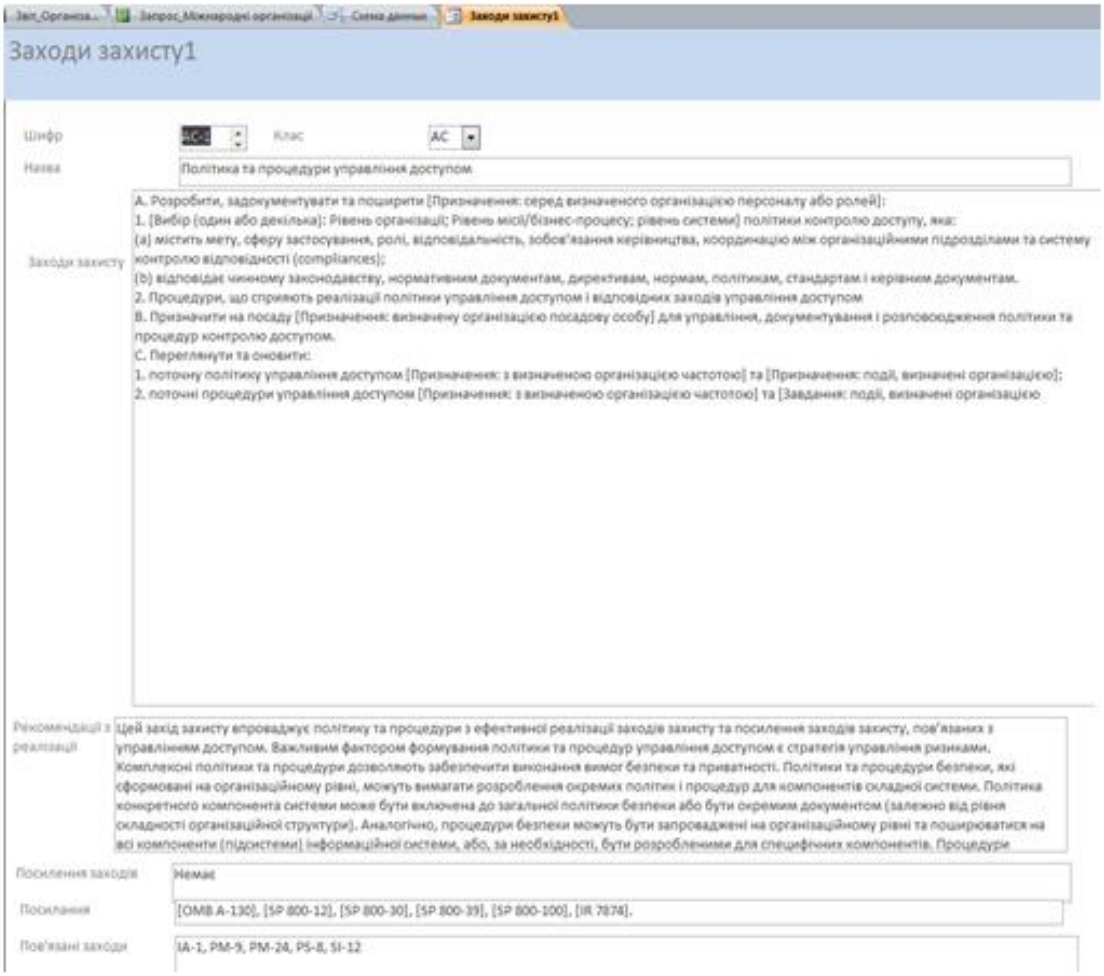


Рисунок 4.26 – Відображення у формі «Заходи захисту» засобу захисту, що не має посилень

Таблиця «Заходи захисту» в режимі таблиці наведена на рис.4.27. На рис.4.28 представлено відображення у формі «Заходи захисту» засобу захисту, що має декілька посилень.

Шифр	Клас	Назва	Заходи захисту	Рекомендації з реалізації	Посилен	Посилання	Пов'язані заходи
AC-1	AC	Політика та процедури управління доступом	A. Розробити, задокументувати та поширити [Призначення: серед визначеного організацією персоналу або ролей]: 1. [Вибір (один або декілька): Рівень організації; Рівень місії/бізнес-процесу; рівень системи] політики контролю доступу, яка: (a) містить мету, сферу застосування, ролі, відповідальність, зобов'язання керівництва, координацію між організаційними підрозділами та систему контролю відповідності (compliances); (b) відповідає чинному законодавству, нормативним документам, директивам, нормам, політикам, стандартам і керівним документам. 2. Процедури, що сприяють реалізації політики управління доступом і відповідних заходів управління доступом B. Призначити на посаду [Призначення: визначену організацією посадову особу] для управління, документування і розповсюдження політики та процедур контролю доступом. C. Переглянути та оновити: 1. поточну політику управління доступом [Призначення: з визначеною організацією частотою] та [Призначення: події, визначені організацією]; 2. поточні процедури управління доступом [Призначення: з визначеною організацією частотою] та [Завдання: події, визначені організацією	Цей захід захисту впроваджує політику та процедури з ефективної реалізації заходів захисту та посилення заходів захисту, пов'язаних з управлінням доступом. Важливим фактором формування політики та процедур управління доступом є стратегія управління ризиками. Комплексні політики та процедури дозволяють забезпечити виконання вимог безпеки та приватності. Політики та процедури безпеки, які сформовані на організаційному рівні, можуть вимагати розроблення окремих політик і процедур для компонентів складної системи. Політика конкретного компонента системи може бути включена до загальної політики безпеки або бути окремим документом (залежно від рівня складності організаційної структури). Аналогічно, процедури безпеки можуть бути запроваджені на організаційному рівні та поширюватися на всі компоненти (підсистеми) інформаційної системи, або, за необхідності, бути розробленими для специфічних компонентів. Процедури мають описувати спосіб реалізації політик, а також засоби контролю за їх виконанням. Процедури можуть бути задокументовані в планах захисту інформації та персональних даних або в окремих документах. Події, які можуть спричинити оновлення політики та процедур контролю доступу, включають висновки оцінки або аудиту, інциденти чи порушення безпеки або зміни в законах, розпорядженнях, директивах, постановах, політиках, стандартах і вказівках. Просте повторне встановлення засобів контролю не є заходом чи процедурою організаційної політики	Немає	[OMB A-130], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100], [IR 7874].	IA-1, PM-9, PM-24, PS-8, SI-12
AC-2	AC	Управління обліковими	A. Визначити та задокументувати типи облікових записів системи, дозволених для використання в ІС для підтримки	Типи облікових записів системи містять, наприклад, індивідуальний, спільний, типовий, системний, гостьовий	AC-2(1), AC-2(2),	[SP 800-162], [SP 800-178]	AC-3, AC-5, AC-6, AC-17, AC-18, AC-

Рисунок 4.27 – Фрагмент таблиці «Заходи захисту» в режимі таблиці

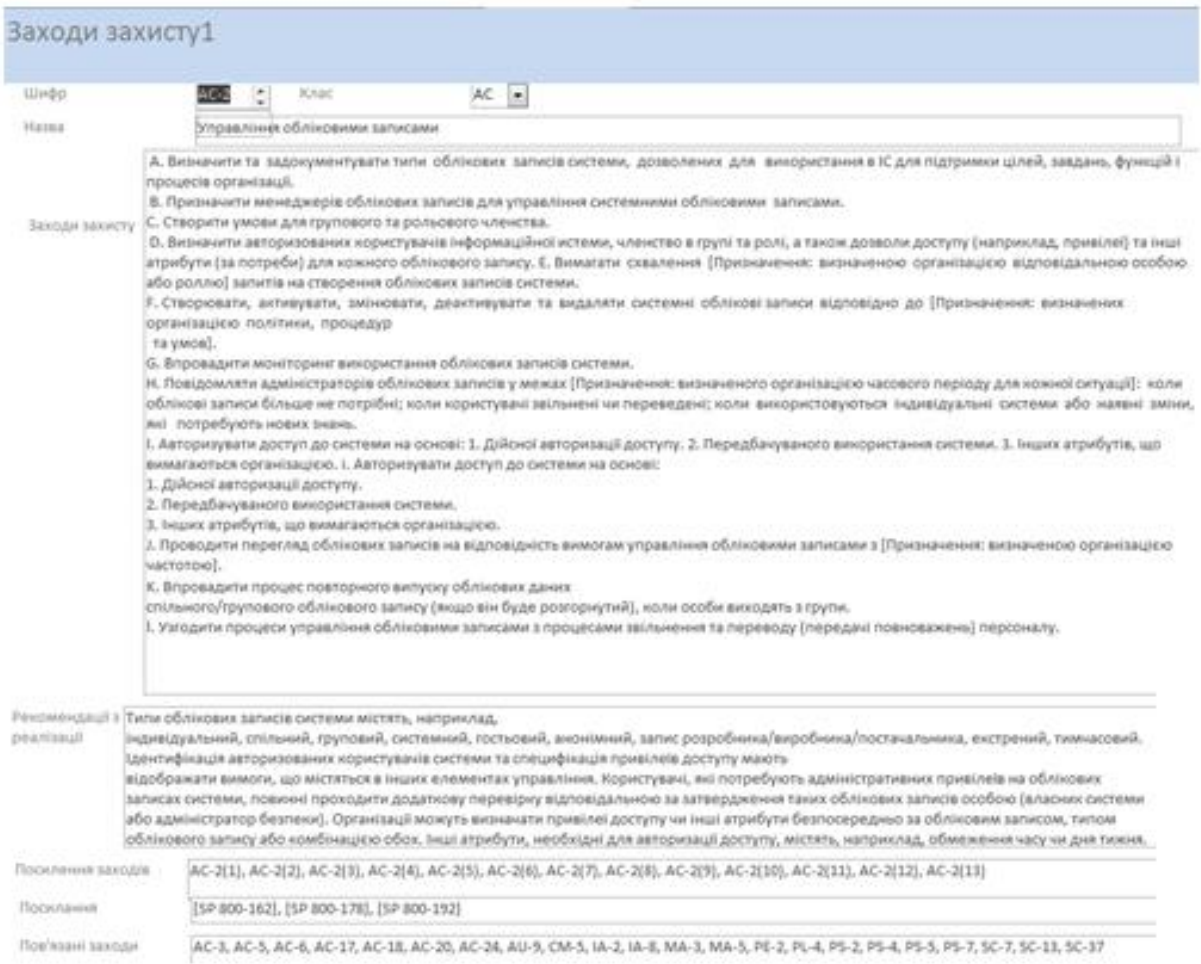


Рисунок 4.28 – Відображення у формі «Заходи захисту» засобу захисту, що має низку посилень

Посилення, наявні в різній кількості у різних засобів захисту, представлені в таблиці «Посилення заходів захисту» (рис.4.29, 4.30), за якою була створена відповідна форма (рис.4.31, 4.32).

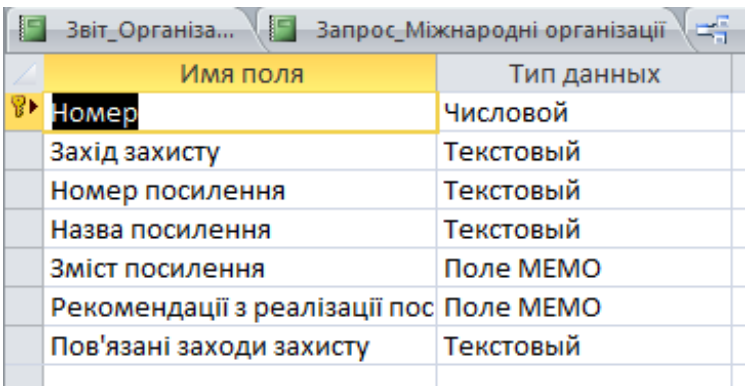


Рисунок 4.29 – Таблиця «Посилення заходів захисту» в режимі конструктора

Звіт_Організа... | Запрос_Міжнародні організації | Схема данных | Посилення заходів захисту

Номер	Захід	Номер	Назва посилення	Зміст посилення	Рекомендації з реалізації посилення	Пов'язані заходи захисту
1	AC-1	не має				Немає
2	AC-2	(1)	Автоматизоване управління системними обліковими записами	Використовувати автоматизовані механізми для підтримки управління системними обліковими записами	Використання автоматизованих механізмів може охоплювати, наприклад, використання електронної пошти чи текстових повідомлень для автоматичного сповіщення менеджерів облікових записів про припинення роботи користувачів; використання системи моніторингу активності облікових записів і використання телефонного сповіщення для повідомлення про нетипове використання облікового запису	Немає
3	AC-2	(2)	Видалення тимчасових та екстренних облікових записів	Автоматично [Вибір: видаляти, деактивувати] тимчасові та екстрені облікові записи після [Призначення: визначеного організацією часового періоду для кожного типу облікових записів]	Це посилення вимагає автоматичного видалення або деактивацію тимчасових і екстрених облікових записів після того, як минув попередньо визначений період часу, без участі системного адміністратора. Автоматичне видалення або деактивація облікових записів забезпечує послідовну реалізацію політики управління обліковими записами.	Немає

Рисунок 4.30 – Фрагмент таблиці «Посилення заходів захисту» в режимі таблиці

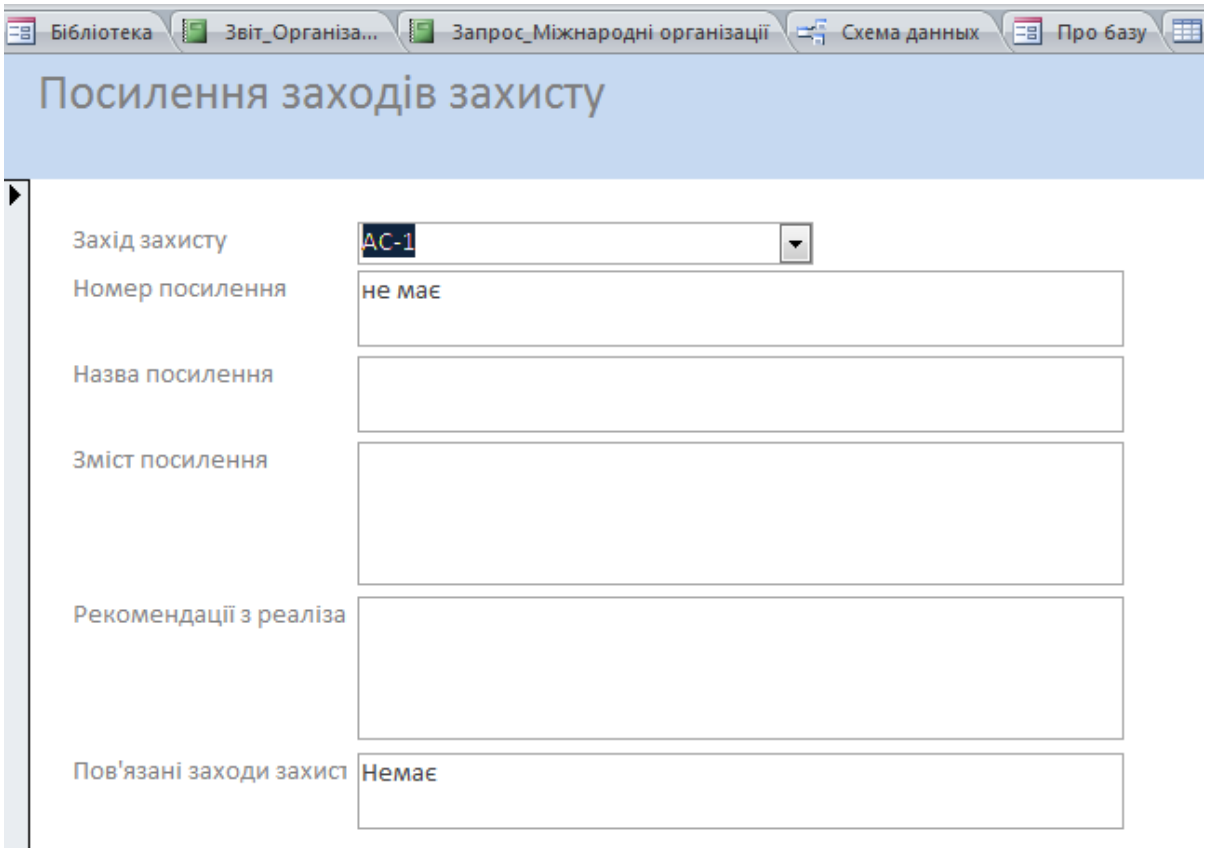


Рисунок 4.31 – Запис у формі «Посилення заходів захисту» для заходу, що не має посилень

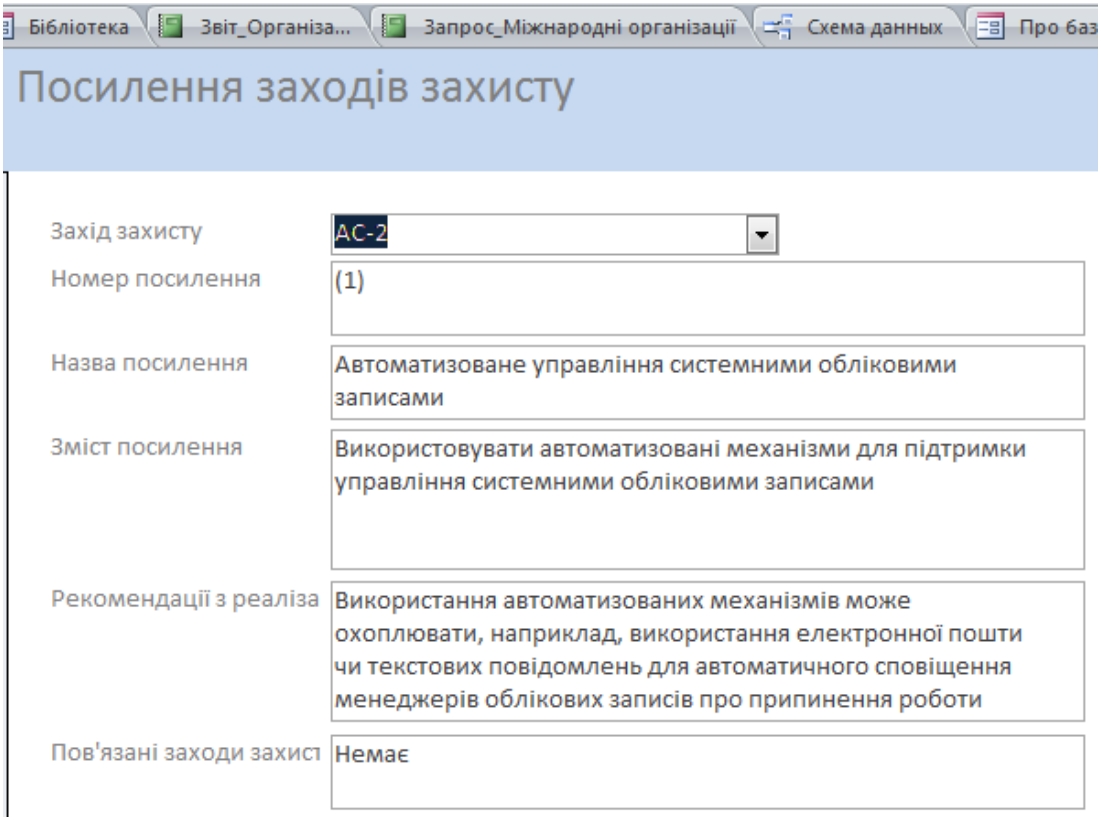


Рисунок 4.32 – Запис у формі «Посилення заходів захисту» для заходу, що має посилення

На рис.4.33 наведена таблиця «Вимоги з безпеки інформації» в режимі таблиці під час її заповнення. В полі «Група вимог» здійснюється підстановка з поля «Назва класу» таблиці «Класи заходів захисту».

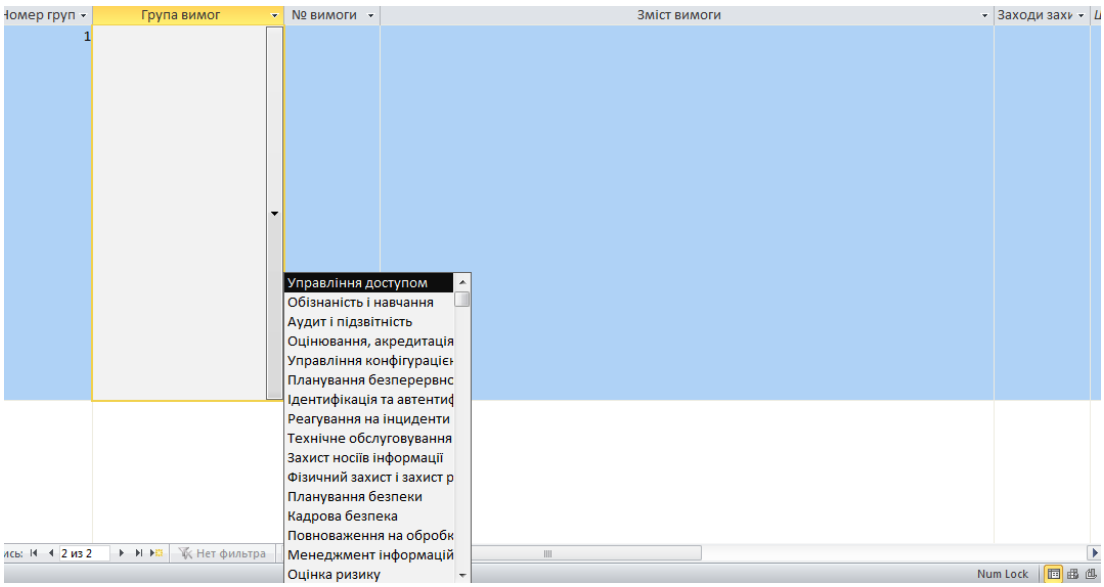


Рисунок 4.33 – Запис у таблицю «Вимоги з безпеки інформації» з підстановкою

На рис.4.34 наведено фрагмент результатів запиту «Вимоги» до взаємопов’язаних таблиць, а на рис 4.35 – звіт, створений за запитом «Заходи-Вимоги».

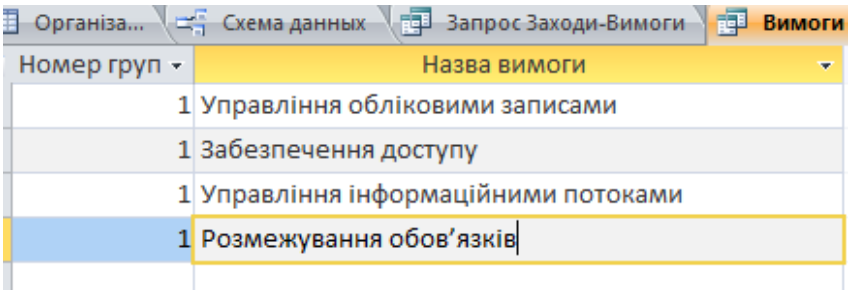


Рисунок 4.34 – Фрагмент результатів запиту «Вимоги»

Рисунок 4.35 – Фрагмент результатів звіту за запитом «Заходи-Вимоги»

ВИСНОВКИ

В даній кваліфікаційній роботі:

− проведено аналіз відкритих літературних джерел і визначений склад бібліотеки нормативно-правових актів та рекомендацій стосовно КСЗІ ОІД у галузі водного транспорту;

− визначений склад документів, які мають бути оформлені в процесі створення КСЗІ ОІД;

− проведено аналіз структури документів, які мають бути оформлені в процесі створення КСЗІ ОІД, визначені типові для них і повторювані блоки інформації та розроблені шаблони документів.

Робота має практичне значення, оскільки її результати можуть бути використані в навчальному процесі зі спеціальності F5 «Кібербезпека та захист інформації» і при проектуванні КСЗІ у галузі водного транспорту.

ПЕРЕЛІК ПОСИЛАНЬ

1. *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive). O.J. L 333, 27.12.2022, p. 80–152. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj*

2. *European Programme for Critical Infrastructure Protection. An official website of the European Union URL: https://eur-lex.europa.eu/EN/legal-content/summary/european-programme-for-critical-infrastructure-protection.html*

3. *IACS E22. Computer-based systems URL: https://www.classnk.or.jp/hp/pdf/info_service/iacs_ur_and_ui/ur_e22_rev.3_june_2023_ul.pdf*

4. *IACS UR E26 Cyber resilience of ships URL: https://www.classnk.or.jp/hp/pdf/info_service/iacs_ur_and_ui/ur_e26_rev.1_nov_2023_cr.pdf*

5. *IACS UR E27 Cyber resilience of on-board systems and equipment. URL: https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/05/29103854/UR-E27-Rev.1-Sep-2023-UL.pdf*

6. *IAPH Cybersecurity Guidelines for Ports and Port Facilities. URL: https://sustainableworldports.org/wp-content/uploads/IAPH-Cybersecurity-Guidelines-version-1_0.pdf*

7. *ISO* 7498-2-89 *Information proceeding systems. Open Systems Interconnection. Basic Reference Model. Part 2: Security Architecture. URL*: *http://www.iso.org/ru/stansard/14256.html*

8. ISO/IEC 17799:2005. *Information technology. Security techniques. Code of practice for information security management. URL: https://www.iso.org/standard/39612.html.*

9. *Good Governance for Critical Infrastructure Resilience. OECD Reviews of Risk Management Policies URL: https://www.oecd.org/content/dam/oecd*

/en/publications/reports/2019/04/good-governance-for-critical-infrastructure-resilience_7d5a9993/02f0e5a0-en.pdf

10. *Limba T., et al. Cyber security management model for critical infrastructure.* (2019). *International Journal Entrepreneurship and Sustainability. Issues ISSN* 2345-0282 *(online). URL: http://jssidoi.org/jesi/ 2017 Volume 4 Number 4 (June). URL: http://doi.org/10.9770/jesi.2017.4.4(12)*

11. *MSC.*428(98). *Maritime cyber risk management in safety management systems: resolution IMO*, прийнята 16.06.2017. *URL: https://www.dohle-yachts. com/wp-content/uploads/2021/05/MSC.42898-2.pdf*

12. *MSC-FAL.1/Circ.3/Rev.2 Guidelines on maritime cyber risk management. URL: https://wwwcdn.imo.org/localresources/en/OurWork/Security/ Documents/ MSC-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime %20Cyber%20 Risk%20Management%20(Secretariat)%20(1).pdf*

13. *NIS2 Directive | Prepare Your Organization Now. The NIS2 Directive. URL: https://nis2directive.eu*.

14. *Osei-Kyei R. Critical review of the threats affecting the building of critical infrastructure resilience.International Journal of Disaster Risk Reductio. V.*60 (2021): 102316. *URL: https://www.sciencedirect.com/science/article/abs/pii/ S221242092100282X*

15. Protecting the cybersecurity of critical infrastructures and their supply chains. ICC Working Paper. July 2024. *URL: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ICC-2024_Protecting-the-cybersecurity-of-critical-infrastructures-and-their-supply-chains.pdf*

16. *Recommendation on Cyber Resilience No. 166. URL: https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/05/24150438/rec-166-corr2-apr-2022-ul.pdf*

17. *The Guidelines on Cyber Security Onboard Ships. Version 5 (2024). URL: https://www.maritimeglobalsecurity.org/media/g3qlxdaw/2024-11-14-guidelines_on_ cyber_security-v5-final.pdf*

18. *Thomas A. J. Cyber Security Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare. London: CRS Press*, 2015. 346 *p. URL: https://wcu.edu.az/uploads/files/Cyber-security%20Protecting%20Critical%20Infrastructures%20from%20Cyber%20Attack%20and%20Cyber%20Warfare%20(%20PDFDrive%20).pdf*

19. Блінцов В.С., Буруніна Ж. Загрози об’єктам морської критичної інфраструктури України та напрямки досліджень щодо їх нейтралізації. Сучасні проблеми інформаційної безпеки на транспорті: матеріали XII Всеукраїнської науково - технічної конференції з міжнародною участю [Електронний ресурс]. Миколаїв : НУК, 2024. С.3-5.

20. Веремчук В.С. Міжнародно-правове регулювання кібербезпеки у морській галузі: сучасний стан та перспективи розвитку. Вісник Одеського Національного ун-ту. Серія: Правознавство. 2024. Т.26. Випуск 1(38). С.112-117. *URL: https://journals.visnyk-onu.od.ua/index.php/law/article/view/472/462*

21. ДБН А.2.2-3-2014. Склад та зміст проектної документації на будівництво. *URL: https://dbn.co.ua/load/normativy/dbnbn_a_2_2_3_2014/1-1-0-1168*

22. Деякі питання ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України: Постанова Кабінету Міністрів України від 16 листопада 2016 р. №821. *URL: https://zakon.rada.gov.ua/laws/show/821-2016-%D0%BF#Text*

23. Деякі питання об’єктів критичної інформаційної інфраструктури: Постанова Кабінету міністрів України від 9 жовтня 2020 р. №943. *URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#n16*

24. Деякі питання об’єктів критичної інфраструктури: Постанова Кабінету міністрів України від 9 жовтня 2020 р. №1109. *URL: https://zakon.rada.gov.ua/rada/show/1109-2020-%D0%BF#Text*

25. Директива 95/46/ЄС Європейського Парламенту і Ради "Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних" від 24 жовтня 1995 року. *URL*: *https://zakon.rada.gov.ua/ laws/show/*994_242

26. Директива 97/66/ЄС Європейського Парламенту і Ради «Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі» від 15 грудня 1997 року. *URL*: *https://zakon. rada.gov.ua/laws/show/*994_243

27. Директива №2002/58/ЄС Європейського Парламенту і Ради ЄС стосовно обробки персональних даних та захисту права на недоторканість особистого життя в сфері електронних комунікацій (Директива про право на недоторканість особистого життя та комунікації, електронні засоби зв'язку). *URL*: *https://zakon.rada.gov.ua/laws/show*/994_*b*34

28. ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення. *URL: http://online.budstandart.com/ua/catalog/dog-page.html?id_doc=61937*

29. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення. *URL: http://metrology.com.ua/ download/dstu-gost-gost-r/60-dstu/441-dstu-3396-0-96*

30. ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт. *URL : http://metrology.com.ua/ download/dstu-gost-gost-r/60-dstu/440-dstu-3396-1-96*

31. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення. *URL: http://www.dut.edu.ua/ru/lib/60 /category/ 925/view/1045*

32. ДСТУ 7731:2015 Інформаційні технології. Методи захисту. Основні положення щодо забезпечення невтручання в особисте життя (ISO/IEC 29100:2011, *MOD*). *URL: https://online.budstandart.com/ua/catalog/doc-page?id_doc=66872*

33. ДСТУ *EN ISO/IEC* 15408-1:2022 Інформаційні технології. Методи захисту. Критерії оцінювання. Частина 1. Вступ та загальна модель (*EN ISO/IEC* 15408-1:2020, *IDT; ISO/IEC* 15408-1:2009, *IDT*). *URL: https://online.budstandart. com/ua/catalog/doc-page.html?id_doc=101797*

34. ДСТУ *EN ISO/IEC* 15408-2:2022 Інформаційні технології. Методи захисту.Критерії оцінювання. Частина 2. Функціональні вимоги (*EN ISO/IEC* 15408-2:2020, *IDT; ISO/IEC* 15408-2:2008, *IDT*). *URL: https://online.budstandart. com /ua/catalog/doc-page.html?id_doc=102013*

35. ДСТУ *EN ISO/IEC* 15408-3:2022 Інформаційні технології. Методи захисту. Критерії оцінювання. Частина 3. Вимоги до гарантії безпеки (*EN ISO/IEC* 15408-3:2020, *IDT; ISO/IEC* 15408-3:2008, *IDT*). *URL: https://online.budstandart.com/ua/catalog/doc-page?id_doc=101798*

36. ДСТУ *ISO* 9001:2015 Системи управління якістю. Вимоги (*ISO* 9001:2015, *IDT*). *URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=64013*

37. ДСТУ *ISO* 14001:2015 Системи екологічного управління. Вимоги та настанови щодо застосовування (*ISO* 14001:2015, *IDT*). *URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=64015*

38. ДСТУ *ISO/IEC* 15408-4:2023 Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 4. Структура для визначення методів оцінювання та діяльності (*ISO/IEC* 15408-4:2022, *IDT*). *URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104389*

39. ДСТУ *ISO/IEC* 15408-5:2023 Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 5. Попередньо визначені пакети вимог до безпеки (*ISO/IEC* 15408-5:2022, *IDT*). *URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104390*

40. ДСТУ *EN ISO/IEC* 18045:2022 Інформаційні технології. Методи захисту. Методологія оцінювання безпеки ІТ (*EN ISO/IEC* 18045:2020, *IDT; ISO/IEC* 18045:2008, *IDT*). *URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=100250*

41. ДСТУ *ISO/IEC* 27000:2019 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів (*ISO/IEC* 27000:2018, *IDT*). *URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85795*

42. ДСТУ *ISO/IEC* 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (*ISO/IEC* 27001:2022, *IDT*). *URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104398*

43. ДСТУ *EN ISO/IEC* 27002:2024 Інформаційна безпека, кібербезпека та захист конфіденційності. Заходи забезпечення інформаційної безпеки (*EN ISO/IEC* 27002:2022, *IDT; ISO/IEC* 27002:2022, *IDT). URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=106958*

44. ДСТУ *ISO/IEC* 27005:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки (*ISO/IEC* 27005:2022, *IDT*). *URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104400*

45. ДСТУ *ISO/IEC* 27035-1:2024 Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 1. Принципи та процес (*ISO/IEC* 27035-1:2023, *IDT*). *URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=112378*

46. ДСТУ *EN ISO/IEC* 29101:2022 Інформаційні технології. Методи захисту. Структура архітектури забезпечення прайвесі (*EN ISO/IEC* 29101:2021, *IDT; ISO/IEC* 29101:2018, IDT). *URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=103346*

47. ДСТУ *ISO* 31000:2018 Менеджмент ризиків. Принципи та настанови (*ISO* 31000:2018, *IDT*). *URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=80322*

48. ДСТУ *EN IEC* 31010:2022 Керування ризиками - методи оцінки ризиків (*EN IEC* 31010:2019, *IDT; IEC* 31010:2019, *IDT*). *URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=100889*

49. Загальні вимоги до кіберзахисту об’єктів КІ, затверджені Постановою Кабінету Міністрів України від 19 червня 2019 р. № 518. *URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text*

50. Звід відомостей, що становлять державну таємницю. *URL: https://zakon.rada.gov.ua/laws/show/z0052-21#n13*

51. Зубков А.П. Критерії прийняття рішень щодо обробки ризиків об’єктів морської інфраструктури. Сучасні проблеми інформаційної безпеки на транспорті: Матеріали XI Всеукраїнської науково-технічної конференції з

міжнародною участю. Миколаїв: НУК, 2023. С.175-181. *URL: https://nuos.edu.ua /wp-content/uploads/2024/03/SPIBT-2023-Materiali.pdf*

52. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних. *URL*: *https://zakon.rada.gov.ua/laws/show*/994_326

53. Конвенція про захист прав людини і основоположних свобод. *URL*: *https://zakon.rada.gov.ua/laws/show/*995_004

54. Конвенція про кіберзлочинність. *URL: https://zakon.rada.gov.ua/laws/ show /994_575#Text*

55. Міжнародна конвенція з охорони людського життя на морі (*SOLAS*-74). *URL: https://zakon.cc/law/document/read/995_251*

56. Наказ Адміністрації Держспецзв'язку від 15.01.2021 №23 «Про затвердження Методичних рекомендацій щодо категоризації об'єктів КІ». *URL: https://zakon.rada.gov.ua/ rada/show/v0023519-21#Text*

57. Наказ Адміністрації Держспецзв'язку від 24.06.2024 № 317 «Про визначення Базового профілю безпеки інформації». *URL: https://cip.gov.ua/ ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-24-06-2024-317-pro-viznachennya-bazovogo-profilyu-bezpeki-informaciyi*

58. Наказ Адміністрації Держспецзв'язку і Служби безпеки України від 19.12.2024 №627/772 «Деякі питання розробки, затвердження та погодження планів захисту об'єктів критичної інфраструктури за проектною загрозою національного рівня «кібератака/кіберінцидент»». *URL: https://cip.gov.ua/services/cm/api /attachment/download?id=66819*

59. Наказ Адміністрації ДССЗЗІ від 26.03.2007 №45 «Про затвердження Порядку оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації». *URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/ publish/ article?art_id=50825&cat_id=38835*

60. Наказ Міністерства оборони України від 17.10.2023 №605 «Про затвердження Переліку відомостей Міністерства оборони України, які містять

службову інформацію (ПСІ-2023)». *URL: https://zakon.rada.gov.ua/rada/show/v0605322-23#Text*

61. Наказ Служби безпеки України від 23.12.2020 №383 «Про затвердження Зводу відомостей, що становлять державну таємницю». *URL: https://zakon.rada.gov.ua/laws/show/z0052-21#n13*

62. НД ТЗІ 1.4–001-2000 Типове положення про службу захисту інформації в автоматизованій системі. *URL: https://tzi.com.ua/downloads/1.4-001-2000.pdf*

63. НД ТЗІ 2.3-025-21. Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем. *URL: https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi2024*

64. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. *URL: http://dstszi.kmu.gov.ua /dstszi/doccatalog/document?id=106342*

65. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. *URL: http://dstszi.kmu.gov.ua/dstszi/control /uk/publish/article;jsessionid=afd6198c23cb1f96abafd7189bbdce03?showhidden=1&art_id=101870&cat_id=89734&ctime=1344501089407*.

66. НД ТЗІ 2.6-004-21. Порядок авторизації безпеки інформаційних систем. *URL: https://cip.gov.ua/services/cm/api/attachment/download?id=65411*

67. НД ТЗІ 3.6-004-21. Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці. *URL: https://cip.gov.ua/services/cm/api/attachment/download?id=53375*

68. НД ТЗІ 3.6-005-21. Порядок категоріювання безпеки інформаційної системи та інформації. *URL: https://cip.gov.ua/services/cm/api/attachment/download?id=53376*

69. НД ТЗІ 3.6-006-24. Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем. *URL: https://cip.gov.ua/services/cm/api /attachment /download?id=64620*

70. НД ТЗІ 3.6-007-21. Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем. *URL: https://cip.gov.ua/services/cm/api /attachment/download?id=53387*

71. НД ТЗІ 3.6-008-21. Порядок моніторингу безпеки інформаційних систем. *URL: https://cip.gov.ua/services/cm/api/attachment /download?id=53390*

72. НД ТЗІ 3.7-003-2023 «Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-комунікаційній системі». *URL: https://www.cip.gov.ua/services/cm/api/attachment/download?id=60385*

73. Нікулін О.С. Розробка шаблону комплексної системи захисту інформації для підприємства припортової галузі. Сучасні проблеми інформаційної безпеки на транспорті: Матеріали IX Всеукраїнської науково-технічної конференції з міжнародною участю. Миколаїв: НУК, 2021. С.78-83. *URL: https://nuos.edu.ua/wp-content/uploads/2022/06/SPIBT-2021_materiali.pdf*

74. Перелік засобів криптографічного захисту інформації, які мають експертний висновок за результатами державної експертизи у галузі КЗІ. *URL: https://cip.gov.ua/services/cm/api/attachment/download?id=66439*

75. Перелік засобів ТЗІ, які мають експертний висновок про відповідність вимогам технічного захисту інформації. *URL: https://cip.gov.ua/ services/cm/api/attachment/download?id=66579*

76. План реалізації Стратегії кібербезпеки України. *URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text*

77. Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, затверджене постановою Кабінету Міністрів України від 3 вересня 2014 р. №411. *URL: https://zakon.rada.gov.ua/laws/show/411-2014-%D0%BF#Text*

78. Положення про державну експертизу у сфері технічного захисту інформації, затверджене наказом Адміністрації Держспецзв'язку від 16.05.2007 №93. *URL: http://zakon.rada.gov.ua/laws/show/z0820-07#Text*

79. Положення про організаційно-технічну модель кіберзахисту, затверджене Постановою Кабінету Міністрів України №1426 від 29.12.2021 р. *URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF*

80. Положення про систему управління безпекою судноплавства на морському і річковому транспорті, затверджене Наказом Міністерства транспорту України №904 від 20.11.2003. *URL: https://zakon.rada.gov.ua/laws/show/z1193-03#n16*

81. Порядок функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, затверджений постановою №1295 Кабінету міністрів України від 23.12.2020. *URL: https://zakon.rada.gov.ua /laws/show/1295-2020-%D0%BF*

82. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29.03.06 № 373. *URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text*

83. Президент України Володимир Зеленський підписав Закон № 4336-IX про кіберзахист державних інформаційних ресурсів. *URL: https://cip.gov.ua/ua/news/prezident-ukrayini-volodimir-zelenskii-pidpisav-zakon-4336-ix-pro-kiberzakhist-derzhavnikh-informaciinikh-resursiv*

84. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури: Закон України. *URL: https://zakon.rada.gov.ua/laws/show/4336-20#Text*

85. Про внесення змін до нормативного документа системи технічного захисту інформації НД ТЗІ 2.3-025-21: Наказ Адміністрації Держспецзв'язку від 26.09.2024 №531. *URL: https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-26-09-2024-531-pro-vnesennya-zmin-do-normativnogo-dokumenta-sistemi-tekhnichnogo-zakhistu-informaciyi-nd-tzi-2-3-025-21*

86. Про внесення змін до Постанови Кабінету Міністрів України від 9 жовтня 2020 р. № 1109. Постанова Кабінету міністрів України №48 від 16 січня 2024 р. *URL: https://zakon.rada.gov.ua/laws/show/48-2024-%D0%BF#Text*

87. Про державну таємницю: Закон України. *URL: https://zakon.rada. gov.ua /laws/show/3855-12#Text*

88. Про затвердження переліку внутрішніх морських вод і внутрішніх водних шляхів, віднесених до категорії судноплавних. Постанова Кабінету Міністрів України від 9 лютого 2022 р. №136. *URL: https://zakon.rada.gov.ua/ laws/show/136-2022-%D0%BF#Text*

89. Про затвердження плану заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України. Розпорядження № 1163-р Кабінету міністрів України від 19 грудня 2023 р. *URL: https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Text*

90. Про затвердження Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб: Наказ Адміністрації ДССЗЗІ 18.10.2023 № 899. *URL: https://zakon.rada.gov.ua/laws/show/z2091-23#Text*

91. Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури: Постанова Кабінету міністрів України від 22 липня 2022 р. №821. *URL: https://zakon.rada. gov.ua/ laws/show/821-2022-%D0%BF#n8*

92. Про затвердження Рекомендацій з оцінки достатності заходів захисту інформації комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації: Наказ Адміністрації Держспецзв'язку №354 від 10.07.2024. *URL: https://zakon.rada.gov.ua/rada/ show/v0354519-24#Text*

93. Про захист інформації в інформаційно-комунікаційних системах: Закон України. *URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text*

94. Про заходи високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу: Директива Європейського Парламенту та Ради (ЄС) 2016/1148 від 06 липня 2019 року. *URL: https://zakon.rada.gov.ua /rada/show/984_013-16#*

95. Про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту.

Директива Ради 2008/114/ЄС від 08 грудня 2008 року. *URL: https://zakon.rada.gov.ua/ rada/ show/984_002-08#n4*

96. Про критичну інфраструктуру: Закон України. *URL: https://zakon.rada.gov.ua/ laws/show/1882-20#Text*

97. Про основні засади забезпечення кібербезпеки України: Закон України. *URL: https://zakon.rada.gov.ua/laws/show/2163-19*

98. Про схвалення Національної транспортної стратегії України на період до 2030 року. Розпорядження Кабінету Міністрів України від 30 травня 2018 р. №430-р. *URL: https://zakon.rada.gov.ua/laws/show/430-2018-%D1%80?find=1 &text=%D0%BA%D1%96%D0%B1%D0%B5%D1%80#w1_1*

99. РД 50-34.698-90. Автоматизовані системи. Вимоги до змісту документів. *URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=103910*

100. Рекомендації з оцінки достатності заходів захисту інформації комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації, затверджені Наказом Адміністрації Держспецзв'язку №354 від 10.07.2024. *URL: https://zakon.rada.gov.ua/rada/show/v0354519-24#Text*

101. Стратегія кібербезпеки України. Безпечний кіберпростір – запорука успішного розвитку країни. *URL: https://zakon.rada.gov.ua/laws/show/447 /2021#Text*

102. Турти М.В Зважене оцінювання критичності об'єктів морського та річкового транспорту. Сучасні проблеми інформаційної безпеки на транспорті: матеріали XII Всеукраїнської науково - технічної конференції з міжнародною участю [Електронний ресурс]. Миколаїв : НУК, 2024. С.22-28.

103. Хван Ю.В. Нормативно-правова база кібербезпеки галузі водного транспорту. Сучасні проблеми інформаційної безпеки на транспорті: матеріали XII Всеукраїнської науково - технічної конференції з міжнародною участю [Електронний ресурс]. Миколаїв : НУК, 2024. С.156-162.